

IGEL Zero HDX

Benutzerhandbuch



Inhaltsverzeichnis

Einleitung

IGEL Thin Clients setzen sich aus aktueller Hardware und einem Embedded-Betriebssystem zusammen, das je nach Produkt auf IGEL Linux oder Microsoft Windows Embedded Standard basiert. Wir tun unser Bestes, um eine hochwertige Gesamtlösung zu liefern und versprechen Service und Support von gleicher Qualität.

Die IGEL Linux Firmware

Die neuen IGEL Zero Clients für Citrix HDX, Microsoft RDS/ RemoteFX oder VMware Horizon liefern ein echtes Zero Client-Erlebnis zum günstigen Preis, vermeiden aber die für Zero Clients anderer Hersteller typischen Beschränkungen, wie z.B. fehlende Update-Möglichkeit, fehlendes Management und mangelnder Support.

IGEL liefert spezialisierte Zero Clients ohne Kompromisse, d.h. optimiert für je eine der drei führenden Virtualisierungslösungen, und das mit kostenlosem Support. Durch den Appliance Mode booten die Zero Clients schnell und direkt in die jeweilige VDI Session wie Citrix XenDesktop oder VMware Horizon View.

Erleben Sie „Zero Touch Deployment“ durch regelbasierte Konfiguration beim Roll-out. Reduzieren Sie den Managementaufwand durch profilbasiertes, automatisches Remote Management aller Einstellungen auf nahezu null. Für Sie heißt das „Null“ lokales Management.

Die Struktur des IGEL-Setup ist nahezu identisch auf allen Zero Clients und in der Verwaltungssoftware Universal Management Suite (UMS). Konfigurationsparameter können also im lokalen Setup des Geräts an der gleichen Stelle der Baumstruktur gefunden werden wie z. B. in einem Profil der Verwaltungssoftware. Die IGEL Universal Management Suite steht für jeden Kunden auf der IGEL-Downloadseite zur Verfügung und erlaubt die Verwaltung einer unbegrenzten Anzahl an IGEL-Thin Clients.

IGEL Zero Clients sind zukunftssicher. Durch kostenlose Updates erhalten Sie bei Bedarf Zugriff auf neue Funktionalitäten. Und sollten Sie sich später einmal für einen Wechsel der VDI-Lösung entscheiden, dann ist das kein Problem. Mit einer IGEL Universal Desktop Upgradelizenz machen Sie Ihre vorhandene IGEL Zero Client-Hardware fit für den Zugriff auf andere VDI-Lösungen.

1. Schnellinstallation

So installieren Sie den Thin Client innerhalb weniger Minuten in Ihrer Netzwerkumgebung:

1. Verbinden Sie den Thin Client mit einem Monitor (VGA, DVI, DisplayPort), einer AT-kompatiblen Tastatur mit PS/2- oder USB-Anschluss, einer USB-Maus und über eine RJ45-Steckverbindung mit dem LAN.
2. Schließen Sie den Thin Client an die Stromversorgung an.
3. Starten Sie den Thin Client und warten Sie, bis die grafische Benutzeroberfläche geladen ist.
4. Klicken Sie in der Taskleiste das Symbol **Setup** an, alternativ starten Sie das IGEL Setup über die Tastaturkombination Strg+Alt+s.
5. Bestimmen Sie unter **User Interface→Language** die Systemsprache und die Tastaturbelegung.
6. Wählen Sie unter **User Interface→Display** die Anzeigeauflösung.
7. Tragen Sie im Abschnitt **Netzwerk** des Setups eine lokale IP-Adresse ein.

   oder behalten Sie den standardmäßigen DHCP-Modus für die automatische Netzwerkkonfiguration bei.
8. Klicken Sie **OK** zum Speichern und bestätigen Sie die Übernahme der Änderungen.

   Das Gerät wird jetzt ggf. neu gestartet und verwendet nach dem Neustart die neuen Einstellungen.

Für nahezu jede Einstellung ist eine nützliche Kurzinformation (Tooltip) verfügbar. Wenn Sie mehr über eine Einstellung oder eine Option erfahren möchten, positionieren Sie den Mauszeiger darauf und warten einen kurzen Moment. Das Verhalten der Tooltips können Sie unter **Benutzeroberfläche→Bildschirm→Desktop** konfigurieren.

1.1. Der IGEL Linux Desktop

Nach dem Systemstart sehen Sie den Desktop des IGEL Linux.



Figure 1: IGEL Linux Desktop

In der Taskleiste am unteren Bildschirmrand befinden sich folgende Elemente:

- **Startmenü** (auch IGEL-Menü)
- **Schnellstartleiste** mit Symbolen für **Starter für Sitzungen, Setup** und Sitzungen
- **Infobereich** mit Symbolen für **Lautstärke**, **Netzwerk**, **Uhr** und **Desktop** (Fenster verstecken/einblenden)

Das Startmenü bietet folgende Bereiche und Funktionen:

- **Anwendungsbereich** zum Starten von Sitzungen
- **Systembereich** für den Zugriff auf Systemprogramme
- **Infobereich (Über)** zur Anzeige aller relevanten Systeminformationen
- **Suche** zum Auffinden von Funktionen im Startmenü
- Schaltflächen zum **Herunterfahren** und **Neustart** des Systems

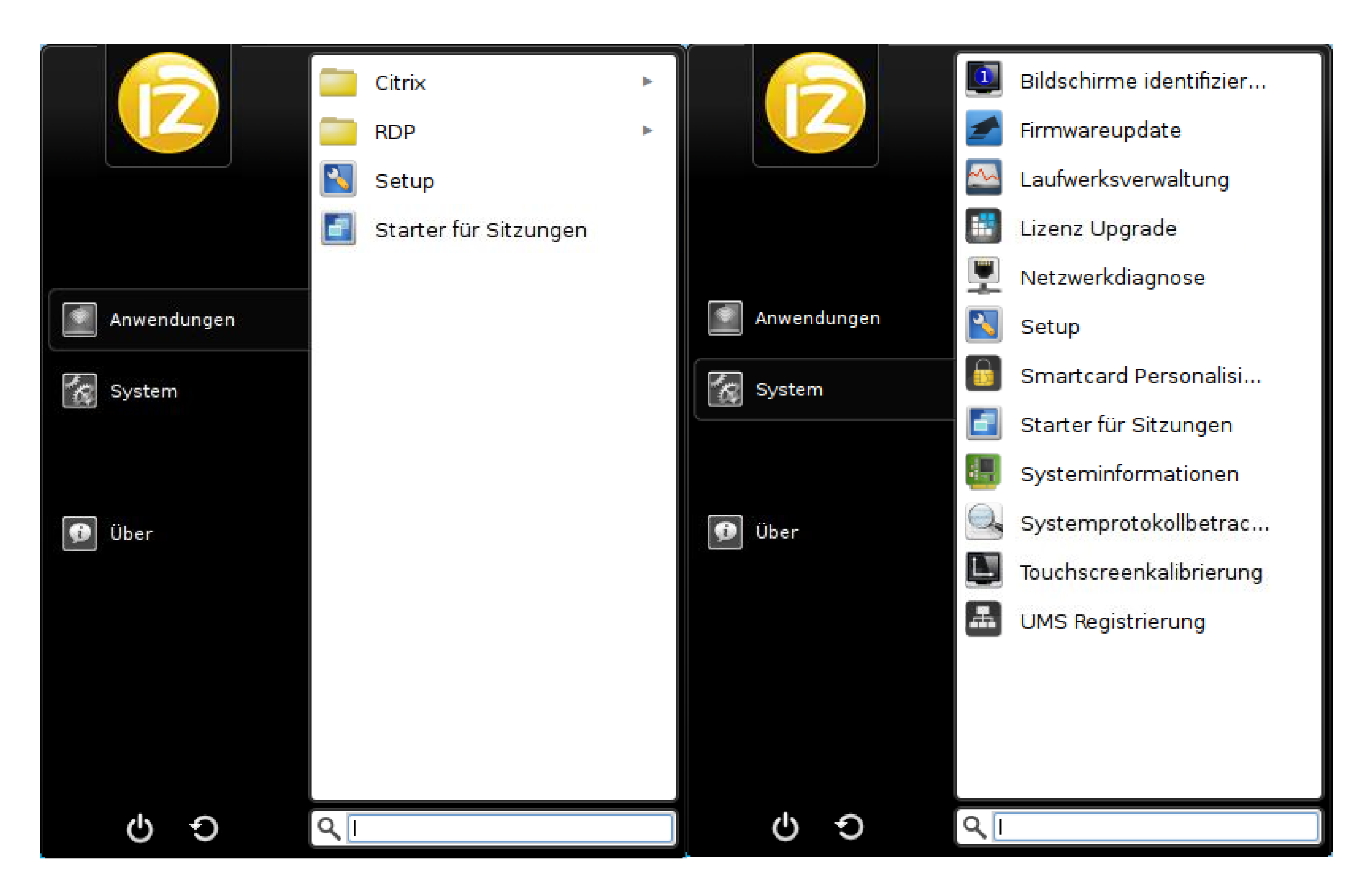


Figure 2: IGEL Startmenü mit Anwendungs- und Systembereich

2. Bootvorgang

Die Schnellinstallation haben Sie erfolgreich durchgeführt.

- Führen Sie einen Neustart durch, um den Bootvorgang zu starten.

2.1. Bootmenü

Während des Bootvorgangs steht Ihnen auf Anforderung ein Bootmenü zur Verfügung, über welches Sie im Fall einer Fehlkonfiguration des Thin Clients und bei Bootproblemen auf Systemparameter zugreifen oder den Thin Client auf Werkseinstellungen zurücksetzen können.

- Drücken Sie während des Startvorgangs die ESC-Taste im **Secondstage Loader** wenn die Meldung **Loading Kernel** auf dem Bildschirm angezeigt wird.

  Es öffnet sich ein Menü mit vier Bootoptionen sowie die Option zum Zurücksetzen des Thin Clients auf die Werkseinstellungen:

Quiet Boot **(Seite 9)**	Normaler Start
Verbose Boot **(Seite 9)**	Start mit Systemmeldungen
Emergency Boot **(Seite 9)**	nur Setup
Failsafe Boot **(Seite 10)**	mit CRC-Check
Reset to Factory Defaults **(Seite 10)**	Zurücksetzen auf Werkseinstellung

2.1.1. Quiet Boot

Quiet Boot ist der standardmäßige Bootmodus. Hierbei werden alle Meldungen des Kernels unterdrückt, und die grafische Benutzeroberfläche wird gestartet.

2.1.2. Verbose Boot

Beim Modus **Verbose Boot** werden im Gegensatz zum **Quiet Boot** die Bootmeldungen angezeigt. Außerdem steht eine Diagnose-Shell zur Verfügung, von der aus gängige Befehle für die Fehlersuche und -beseitigung (wie ifconfig usw.) ausgeführt werden können.

- Geben Sie `init 3` ein, um diese Shell zu schließen.

  Der Bootvorgang wird fortgesetzt.

2.1.3. Emergency Boot

Emergency Boot ist ein Setup mit Standardparametern.

Wenn Sie **Emergency Boot** auswählen, sucht der Secondstage Loader im Flashspeicher nach einem bootfähigen System und setzt den Bootvorgang wie in den anderen Bootmodi fort.

Im Wesentlichen wird bei einem **Emergency Boot** der X-Server ohne Netzwerktreiber mit einer Auflösung von 640 x 480 - 60 Hz gestartet. Dann wird direkt das Menü **Setup** geöffnet.

Diese Option ist z. B. nützlich, wenn Sie eine zu hohe Bildschirmauflösung oder einen falschen Maustyp ausgewählt haben und Sie diese im normalen Setup nicht mehr ändern können.

2.1.4. Failsafe Boot - CRC-Check

Beim **Failsafe Boot** wird zunächst eine Prüfung des Dateisystems durchgeführt, anschließend startet der Thin Client im **Verbose-Modus**.

2.1.5. Reset to Factory Defaults

Beim **Zurücksetzen auf Werkseinstellungen** gehen alle persönlichen Einstellungen auf dem Thin Client verloren, darunter auch Ihr Passwort und Ihre konfigurierten Sitzungen.

Bevor der Vorgang ausgeführt wird, wird auf dem Bildschirm eine Warnmeldung angezeigt.

- Bestätigen Sie Ihre Entscheidung.

Wenn das Gerät durch ein Administratorpasswort geschützt ist, werden Sie aufgefordert, dieses Passwort einzugeben. Sie haben dafür drei Versuche.

Ist das Passwort nicht bekannt?

1. Drücken Sie bei der Passwortabfrage dreimal die Eingabetaste.
2. Drücken Sie c, um sich den **Terminal Key**, den individuellen Schlüssel des Thin Clients, anzeigen zu lassen.
3. Wenden Sie sich an uns per *IGEL Service RMA-Formular https://www.igel.com/de/service-support/rma-anforderung-ruecksendung.html*.
4. Geben Sie den angezeigten **Terminal Key** und die angegebene Firmwareversion sowie Ihre Kontaktdaten an.

Unser Service wird Ihnen einen so genannten Reset to Factory Defaults Key - Schlüssel zum Zurücksetzen - speziell für Ihr Gerät übermitteln. Jeder Key gilt nur für je ein Gerät, um den Vorgang so einfach wie möglich und trotzdem sicher zu gestalten.

2.2. Netzwerkintegration

Ist der Kernel geladen?

Dann folgt nun die Netzwerkkonfiguration.

Es stehen drei verschiedene Möglichkeiten zur Auswahl, um das Terminal in die Netzwerkumgebung zu integrieren. In Abhängigkeit von den Einstellungen des Terminals kann zwischen **DHCP**, **BOOTP** oder einer **manuell eingerichteten IP-Adresse** gewählt werden.

Das Netzwerkinterface lässt sich auf der Linux Konsole (erreichbar über Strg+Alt+F11) mit diesem Befehl beenden und neu starten:

```
/etc/init.d/network stop
/etc/init.d/network start
```

2.3. X-Server

Im letzten Schritt des Bootvorgangs werden der X-Server und der lokale Windowmanager gestartet.

Bei Anzeigeproblemen oder nicht mehr reagierender grafischer Oberfläche können Sie den X-Server über die Tastenkombination Alt+Druck+k neu starten.

3. Starter für Sitzungen

- Klicken Sie das Symbol **Starter für Sitzungen** (Application Launcher) in der Schnellstartleiste oder im Startmenü, um das Tool zu starten.

Die verschiedenen Unterbereiche des Starters erlauben den Zugriff auf eingerichtete Sitzungen, Systemprogramme oder zeigen Informationen zu Lizenzen, System und Netzwerkverbindungen an.



Figure 3: Starter für Sitzungen

Da das Setupprogramm das zentrale Konfigurationstool für alle Einstellungen des Thin Clients ist, ist eine Setupsitzung bereits unter **Sitzungen** und **System** vordefiniert.

Sitzungen (Seite 22)

System (Seite 14)

Lizenz (Seite 15)

Informationen

Netzwerk Informationen (page 16)

Herunterfahren und Neustart (Seite 16)

3.1. Allgemeine Systeminformationen

Im **Starter für Sitzungen** finden Sie die Seite **Informationen** mit wichtigen Daten zum System wie Firmwareversion, lizenzierte Services und Hardwarespezifikationen.



Figure 4: Starter für Sitzungen - Systeminformationen

Auch die aktuelle Netzwerkkonfiguration mit IP-Adresse und Gerätenamen ist hier aufgeführt.

3.2. Sitzungen

Alle angelegten Sitzungen werden in einer Anwendungsliste aufgeführt, wenn sie für die Sitzungshauptseite aktiviert sind.

- Doppelklicken Sie eine Anwendung oder klicken Sie **Ausführen**, um sie zu öffnen.
- Alternativ können Sie Sitzungen über Icons auf dem Desktop, in der Schnellstartleiste oder aus dem Startmenü und Kontextmenü heraus starten.
- Auch ein automatischer Start von Anwendungen und die Definition einer Tastenkombination (Hotkey) ist möglich.

> Die verfügbaren Startoptionen einer Sitzung lassen sich in der Sitzungskonfiguration unter **Desktopintegration** festlegen.

3.3. Systemwerkzeuge

Unter **System** können Sie verschiedene Werkzeuge ausführen, z. B. auch die Firmwareaktualisierung mit den voreingestellten Updateinformationen.

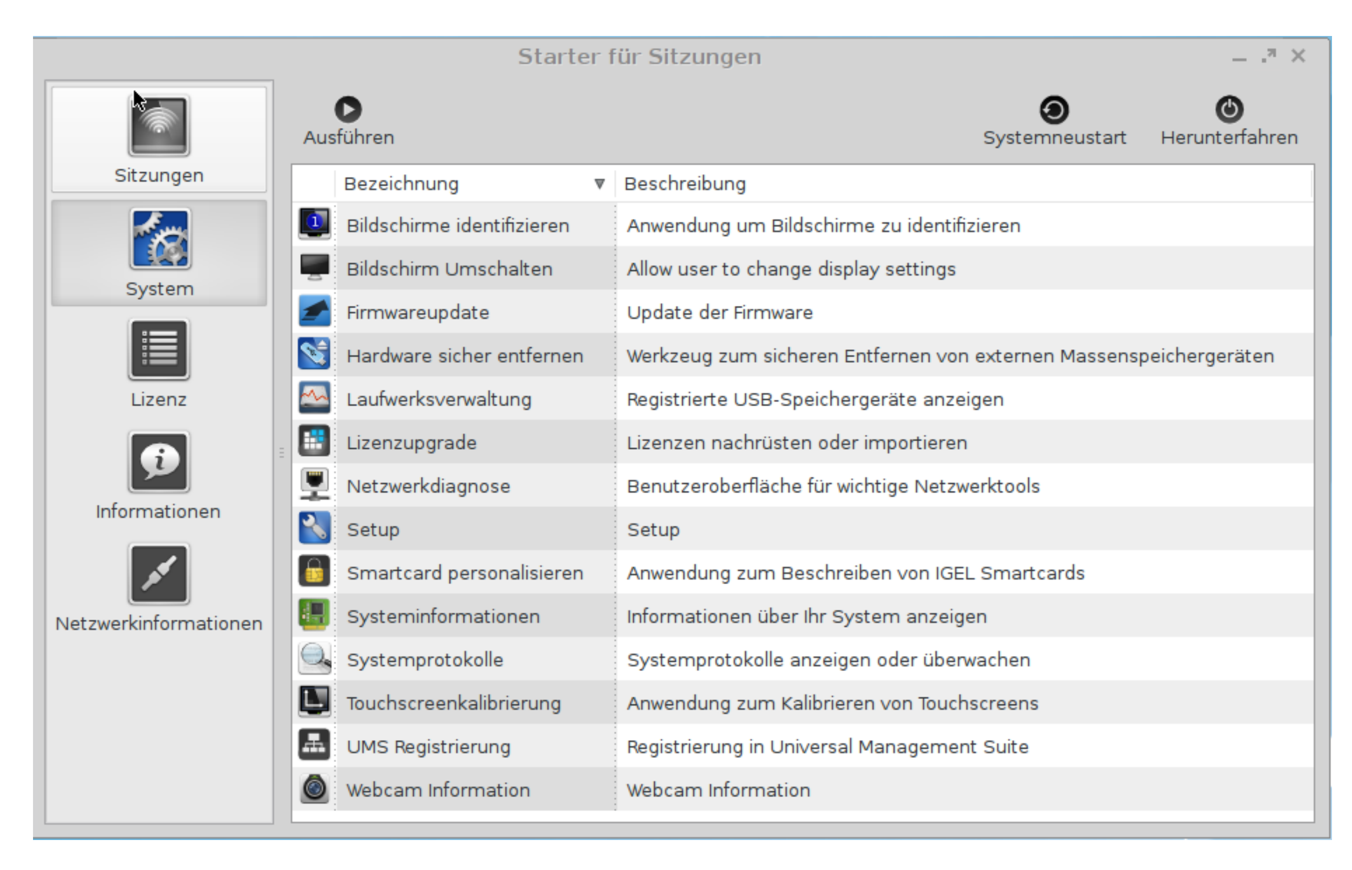


Figure 5: Starter für Sitzungen - Systemwerkzeuge

Die Werkzeuge im Einzelnen:

Bildschirme identifizieren	Zeigt die Nummer und Herstellerdaten des Bildschirms an.
Bildschirm umschalten	Schaltet zwischen mehreren Bildschirmen um.
Firmwareupdate	Führt das Update mit den im Setup hinterlegten Einstellungen aus.
Hardware sicher entfernen	Entfernt externe Speichergeräte ohne Gefahr des Datenverlusts.
Laufwerksverwaltung	Zeigt Informationen zu angeschlossenen USB-Laufwerken an.
Lizenzupgrade	Liest eine neue Lizenzdatei vom USB-Stick und passt den Funktionsumfang der Firmware entsprechend an.
Netzwerkdiagnose	Liefert detaillierte Informationen zur Netzwerkverbindung und bietet einige Tools wie Ping oder Traceroute zur Problemanalyse.
Setup	Startet das IGEL Setup.
Smartcard Personalisierung	Dient zum Beschreiben einer IGEL Smartcard mit Zugangsdaten und Sitzungen, die dem Benutzer der Karte zur Verfügung stehen sollen.
Systeminformationen	Zeigt Informationen über Hardware, Netzwerk und angeschlossene Geräte an.
Systemprotokolle	Zeigt Logdateien des Systems "live" an, eigene Logs lassen sich hinzufügen
Touchscreen Kalibrierung	Erlaubt das Kalibrieren eines angeschlossenen Touchscreenmonitors.
UMS-Registrierung	Meldet den Thin Client an einem UMS-Server an, die Zugangsdaten zum Server werden benötigt.
Webcam Information	Zeigt Daten einer angeschlossenen Webcam und ermöglicht den Test der Kamera.

3.4. Lizenz

Hier finden Sie:

- die Lizenzen der im UD-System verwendeten Komponenten
- Informationen zur Bereitstellung von Quellcode, z. B. unter GPL

3.5. Netzwerkinformationen

Mit dem Werkzeug **Netzwerkinformationen** lesen Sie Daten Ihrer lokalen Netzwerkverbindungen aus und prüfen die Verfügbarkeit eines UMS Servers:



Figure 6: Netzwerkinformationen

3.6. Herunterfahren und Neustart

Im **Starter für Sitzungen** finden Sie zwei Schaltflächen zum Starten oder Herunterfahren des Geräts. Beide Aktionen können für den Benutzer deaktiviert werden und stehen dann nur dem Administrator zur Verfügung.

Die Standardaktion beim Herunterfahren über die Schaltfläche oder den Einschaltknopf am Gerät können Sie im Setup ändern unter **System→Energie→Herunterfahren**.

4. Setupanwendung

Mit Hilfe des Setups können Sie Einstellungen an der Systemkonfiguration und an den Sitzungen vornehmen.

Die Einstellungen, die Sie in der UMS vorgenommen haben, sind vorrangig und können eventuell nicht mehr verändert werden. Nicht veränderbare Einstellungen erkennen Sie an dem vorangestellten Schlosssymbol.

4.1. Setup starten

Sie haben folgende Möglichkeiten, das Setup zu öffnen:

- Doppelklicken Sie **Setup** im **Starter für Sitzungen**
  oder klicken Sie **Ausführen**.
- Doppelklicken Sie **Setup** auf dem Desktop (sofern eingerichtet).
- Wählen Sie **Setup** im Kontextmenü des Desktops (sofern eingerichtet).
- Wählen Sie **System→Setup** im Startmenü.
- Klicken Sie **Setup** in der Schnellstartleiste.
- Starten Sie das Setup über das Tastaturkommando Strg+Alt+s,
  im Appliance-Modus über Strg+Alt+F2.

Unter **Zubehör** können Sie konfigurieren, wie das Setup aufgerufen werden kann. Dabei stehen die o.g. Möglichkeiten und beliebige Kombinationen daraus zur Verfügung.

4.2. Setup beenden

Die Schaltflächen **OK**, **Abbrechen** und **Übernehmen** sind üblicherweise auf jeder einzelnen Setupseite vorhanden.

- Klicken Sie **Übernehmen**, wenn Sie alle Konfigurationen in einem Setupbereich vorgenommen haben und Ihre Einstellungen speichern möchten, ohne das Setupprogramm zu schließen.
- Klicken Sie **Abbrechen**, wenn Sie keine Änderungen vorgenommen haben und das Setup abbrechen möchten.

➢ Klicken Sie **OK**, um die Änderungen zu speichern und das Setup zu verlassen.

4.3. Bereiche des Setups

Die Setupanwendung enthält die folgenden Hauptbereiche:



Figure 7: Bereiche des Setups

Sitzungen	Konfigurieren von Anwendungssitzungen verschiedener Sitzungstypen
Zubehör	Konfigurieren einiger lokaler Tools - Setupseiten für die lokale Shell (Terminal), Sound Mixer, Bildschirmtastatur (für Touchscreenmonitore), Optionen für den **Starter für Sitzungen** und die Setupanwendung selbst
Benutzeroberfläche	Konfigurieren von Anzeigeeinstellungen, Eingabegeräten, Hotkeybefehlen usw.
Netzwerk	Konfigurieren aller Netzwerkeinstellungen für LAN/WLAN-Schnittstellen und die Einwahlverbindungen
Geräte	Konfigurieren verschiedener Geräte
Sicherheit	Festlegen der Passwörter für Administrator und Benutzer und der Benutzerberechtigungen usw.
System	Festlegen einiger grundlegender Systemparameter, darunter Datum und Uhrzeit, Informationen zum Firmwareupdate, Remote-Management und andere

➢ Klicken Sie auf einen der Bereiche, um die jeweilige Unterstruktur zu öffnen.

Die Baumstruktur ermöglicht Ihnen, zwischen den Setupoptionen zu wechseln.

Es stehen drei Navigationsschaltflächen zur Verfügung, mit denen Sie zwischen den besuchten Setupseiten hin- und herblättern oder auf die übergeordnete Strukturebene gelangen können.

Eine detailliertere Beschreibung der einzelnen Setupoptionen folgt an anderer Stelle. Dies ist nur ein kurzer Überblick.

4.3.1. Setupseiten für Benutzer freigeben

Wenn für den Administrator ein Kennwort eingerichtet wurde, lässt sich das IGEL Setup nur noch als Administrator nach Eingabe des Kennworts öffnen (siehe *Passwort* (Seite 114)). Einzelne Bereiche des Setups lassen sich aber auch für den Benutzer freischalten, z. B. damit dieser die Systemsprache ändern oder eine Linkshändermaus konfigurieren kann.

1. Aktivieren Sie unter **Sicherheit→Passwort** das Passwort für den **Administrator** und den **Setupbenutzer**.

> Sollen Benutzer Teile des Setups auch ohne Passwort bearbeiten dürfen, legen Sie eine *Quicksetup* (Seite 19) Sitzung an, das Passwort für den **Setupbenutzer** wird in diesem Fall nicht aktiviert.

2. Schalten Sie unter **Zubehör→Setupsitzung→Seitenberechtigungen** diejenigen Bereiche frei, auf welche der Benutzer Zugriff haben soll.
   - Eine aktivierte Checkbox zeigt an, dass der Knoten im Setup sichtbar ist.
   - Ein grünes Symbol (offenes Schloss) zeigt an, dass der Benutzer die Parameter auf dieser Setupseite bearbeiten kann

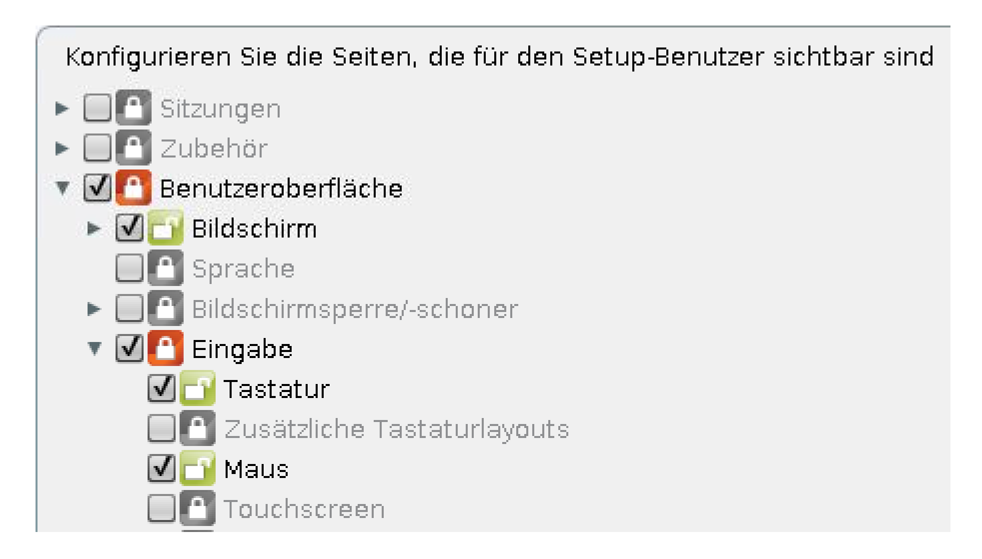


Figure 8: Eingeschränkter Zugriff auf das Setup

> Aktivieren Sie eine Setupseite auf den unteren Ebenen, so werden die für den Zugang notwendigen Knotenpunkte automatisch als sichtbar (aber für die Bearbeitung gesperrt) markiert.

4.3.2. Quicksetup

Wenn für den Administrator ein Kennwort eingerichtet wurde, lässt sich das IGEL Setup nur noch als Administrator nach Eingabe des Kennworts öffnen (siehe *Passwort* (Seite 114)). Einzelne Bereiche des Setups lassen sich aber auch für den Benutzer freischalten, z.B. damit dieser die Systemsprache ändern oder eine Linkshändermaus konfigurieren kann.

1. Aktivieren Sie unter **Sicherheit→Passwort** das Passwort für den **Administrator**.

Sollen Benutzer Teile des Setups nur mit Passwort bearbeiten dürfen, aktivieren Sie auch das Passwort für den **Setupbenutzer**.

2. Definieren Sie unter **Zubehör→Quicksetup** den Namen und die Optionen zum Aufruf des Quicksetups.
3. Schalten Sie unter **Zubehör→Quicksetup→Seitenberechtigungen** diejenigen Bereiche frei, auf welche der Benutzer Zugriff haben soll.
   - Eine aktivierte Checkbox zeigt an, dass der Knoten im Setup sichtbar ist.
   - Ein grünes Symbol (offenes Schloss) zeigt an, dass der Benutzer die Parameter auf dieser Setupseite bearbeiten kann

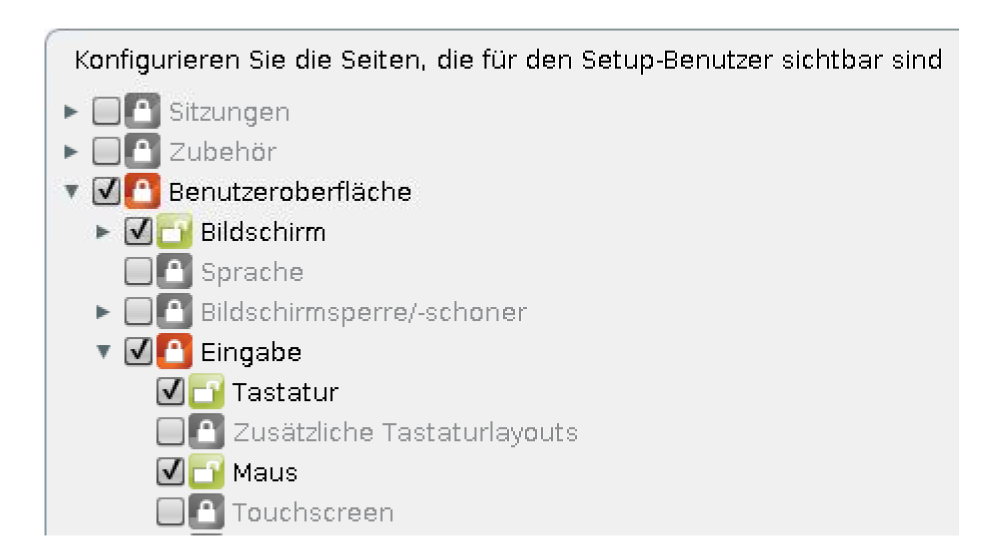


Figure 9: Eingeschränkter Zugriff auf das Setup

Aktivieren Sie eine Setupseite auf den unteren Ebenen, so werden die für den Zugang notwendigen Knotenpunkte automatisch als sichtbar (aber für die Bearbeitung gesperrt) markiert.

4.4. Suche im Setup

Über **Suche** finden Sie im Setup Parameterfelder oder -werte.

1. Öffnen Sie die Suche über die Schaltfläche unterhalb der Baumstruktur.
2. Geben Sie den zu suchenden Text ein.
3. Definieren Sie Details für die Suche, grenzen Sie die Suche z.B. auf Feldbeschriftungen oder -werte ein.
4. Wählen Sie einen der Treffer aus.
5. Klicken Sie **Ergebnis zeigen**, um auf die zugehörige Setupseite zu gelangen.

Der gefundene Parameter oder Wert wird wie unten dargestellt hervorgehoben.



Figure 10: Suche im Setup

5. Sitzungen

Anwendungssitzungen können in der Unterstruktur **Sitzungen** der IGEL Setupanwendung erstellt und konfiguriert werden. Die **Sitzungsübersicht** bietet einen Überblick über alle verfügbaren Sitzungstypen und bestehenden Sitzungen.

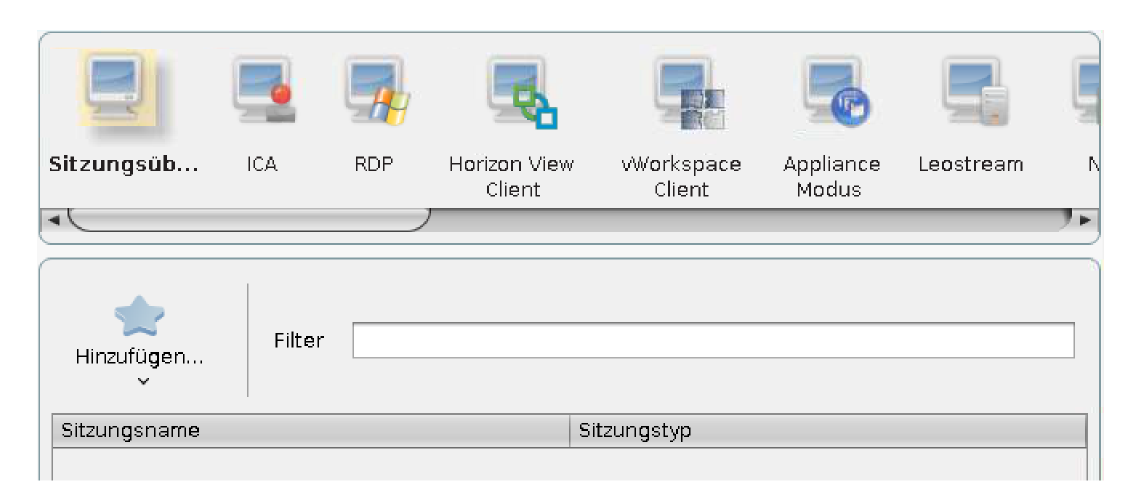


Figure 11: Sitzungsübersicht

➢ Klicken Sie **Hinzufügen**, um eine neue Sitzung zu erstellen.

Deaktivierte Funktionen werden in der Dropdownliste nicht angezeigt.

Für jede Sitzung existiert eine Konfigurationsseite mit dem Seitentitel **Desktopintegration**, auf der Sie folgende Aktionen ausführen können:

- das Erscheinungsbild der Sitzung auf dem lokalen Desktop bestimmen
- den Namen der Sitzung einrichten

> Hinweis: Der Sitzungsname darf keines dieser Zeichen enthalten: \ / : * ? " < > | [ ] { } ( )

- die Sitzungsstartoptionen (Autostart, Neustart) auswählen
- die Hotkeynutzung aktivieren
- ein Passwort zum Starten der Sitzung festlegen (Administrator, Benutzer, Setup Benutzer)

5.1. Citrix Receiverauswahl

Wählen Sie aus, welche der installierten Citrix-Receiverversionen für Citrix-Sitzungen zum Einsatz kommen soll.

> Die vorausgewählte Einstellung **Standard** entspricht nun Citrix Receiver 13.1.3, während zuvor Version 12 die Voreinstellung war.



Figure 12: Citrix Receiver-Auswahl

Einen Überblick über die Features der Versionen gibt ein FAQ-Dokument.

5.2. Citrix ICA - Globale Einstellungen

In diesem Abschnitt wird die Konfiguration der globalen Citrix-Einstellungen beschrieben, die für alle Citrix-Sitzungen gilt.

Dies sind die Standardwerte für alle Citrix-Sitzungen. Die meisten dieser Eigenschaften, insbesondere die Farbtiefe, Auflösung und die Server-IP oder der Servername, können gesondert für jede Sitzung geändert werden.

Beachten Sie, dass einige Konfigurationsoptionen abhängig sind von der gewählten Version des Citrix Receivers. Das IGEL Setup enthält einige Hinweise dazu, ein Funktionsvergleich bei der Versionen ist in den FAQ zu finden: *Citrix Receiver Feature Matrix* (*http://faq.igel.com/otrs-igel/public.pl?Action=PublicFAQZoom;ItemID=619*).

WICHTIG: Citrix Receiver 13.0.x und 13.1.x (Linux) unterstützt nur HTTPS-Verbindungen, während die Standardeinstellung des Citrix-Servers HTTP ist - ein Verbindungsversuch schlägt somit fehl. Am Citrix-Server muss HTTPS aktiviert werden und es muss sichergestellt sein, dass am Thin Client ein gültiges Rootzertifikat der Zertifizierungsstelle (CA) installiert ist. Ein Best Practice Dokument zur Verteilung der Zertifikate ist in der IGEL Knowledge Base verfügbar: *Deploying Trusted Root Certificates* (*http://edocs.igel.com/index.htm#10200413.htm*)

WICHTIG: Citrix Receiver 13.1 unterstützt Kerberos-Passthrough-Authentifizierung nur für Legacy-ICA-Sitzungen, nicht für Storefornt!!

WICHTIG: Benutzer können ein abgelaufenes Passwort nur ändern, wenn diese Option auch am Citrix-Server aktiviert ist. Siehe FAQ *Warning message when changing password* (*http://faq.igel.com/otrs-igel/public.pl?Action=PublicFAQZoom;ItemID=621*).

5.2.1. Serverstandort

Über die Option **Serverstandort** - auch als Serverbrowsing bezeichnet - rufen Sie mit dem Citrix-ICA-Client, der mit dem Netzwerk verbunden ist, eine Liste aller Citrix-Server und aller veröffentlichten Anwendungen auf, die über das Netzwerk erreichbar sind und die das ausgewählte Browsingprotokoll nutzen.

Die Standardfunktionalität für diese Option ist **Auto-Locate** (Broadcast). Mit dieser Funktion sendet der ICA-Client ein „Get nearest Citrix Server"-Paket. Die Adresse des ersten antwortenden Citrix-Servers funktioniert dann als Master-ICA-Browser.

Sie können auch eine gesonderte **Adressliste** für jedes Netzwerkprotokoll festlegen. Dies kann TCP/IP, TCP/IP + HTTP oder SSL/TLS + HTTPS sein.

TCP/IP	Wenn Ihre Netzwerkkonfiguration Router oder Gateways nutzt oder wenn zusätzlicher Netzwerkverkehr durch die Übertragungen vermieden werden soll, können Sie spezielle Serveradressen für die Citrix-Server festlegen, von denen die Liste der verfügbaren Server und/oder veröffentlichten Anwendungen angefordert werden soll.

> Sie können mehrere Adressen in die Adressliste aufnehmen, sodass die Clients auch dann eine Verbindung aufbauen und funktionieren können, wenn ein oder mehrere Server nicht verfügbar sind.

TCP/IP + HTTP	Sie können die Informationen der verfügbaren Citrix-Server und veröffentlichten Anwendungen auch über eine Firewall hinweg abrufen. Dazu nutzen Sie als Server Standort Protokoll TCP/IP + HTTP.

> „TCP/IP + HTTP" Server Location unterstützt die Auto-Locate-Funktion nicht.

SSL/TLS + HTTPS	Secure Sockets Layer- (SSL) und Transport Layer Security-Verschlüsselung (TLS) bieten Serverauthentifizierung, Verschlüsselung von Datenströmen und die Prüfung der Meldungsintegrität.

> Wenn Sie versuchen, eine von SSL/TLS abweichende Verbindung zu einem SSL/TLS-Server herzustellen, werden Sie nicht verbunden. Die Meldung **Verbindung fehlgeschlagen** wird angezeigt.

5.2.2. Lokale Anmeldung

Kerberos Pass-through-Authentifizierung in allen ICA-Sitzungen benutzen	Diese Option aktiviert Single Sign-on für alle ICA-Sitzungen, falls Anmeldung am Thin Client mit AD/Kerberos konfiguriert ist. Auch der Server muss für die Pass-through-Authentifizierung konfiguriert sein. Beim Start der ICA-Sitzungen ist dann keine erneute Benutzername- und Passworteingabe mehr erforderlich, die lokalen Anmeldedaten (Domänenanmeldung) werden in die Sitzungsanmeldung durchgereicht. Nutzen Sie das lokale Anmeldemodul, wenn Probleme mit dem Load Balancing auftreten. Beim Verbinden zum Metaframe-Masterbrowser werden die Anmeldeinformationen des Benutzers übermittelt.
Lokales Anmeldefenster benutzen	Ist diese Option aktiv, müssen Sie für die Anmeldung das Passwort erneut eingeben.
Neustart Modus	Das Anmeldemodul wird automatisch neu gestartet, nachdem es geschlossen wurde.
Typ	Hier können Sie Benutzername und Domäne im Anmeldefenster vorbelegen und zwischen den Einstellungen aus dem letzten Login und dem Sitzungssetup wählen.
Login Informationen vorbelegen	Benutzername und Domäne werden Anmeldefenster vorbelegt.
Domäne anzeigen	Zeigt den Domäneneintrag im Anmeldefenster an.
Clientname als Benutzernamen übernehmen	Diese Einstellung kann ggf. Probleme mit der Wiederverbindung bei Load Balancing beheben.
Anmeldung mit Smartcard ermöglichen	Nur bestimmte Smartcard Typen werden unterstützt, eine Liste der aktivierbaren Typen finden sie im Unterpunkt **Smartcard** des Setups.
Domänen	Hinzufügen der Domänen, die verfügbar sein sollen. Wenn Sie mehrere Domänen eintragen, werden diese im Drop-down-Feld **Domäne** im Anmeldemodul angezeigt.
Smartcard	Ermöglicht den lokalen Zugriff auf Smartcards und Token verschiedener Hersteller.

5.2.3. Fenster

Unter **Fenster** nehmen Sie folgende Konfigurationen vor:

Standardanzahl an Farben	Festsetzen der Standard-Farbtiefe - Die Default-Einstellung ist eine Farbtiefe von 256 Farben.
Farben approximieren	Aufgrund der Unterschiede zwischen den vom ICA-Client und vom „Thin Client“-Desktop verwendeten Farbpaletten kann es zu einem störenden Blinken kommen, wenn zwischen Fenstern auf einem Pseudofarbenbildschirm gewechselt wird. Das Farbangleichungsschema des ICA-Clients vermeidet dieses Blinken, denn es verwendet die Farben der lokalen Desktoppalette, um die ICA-Fenstersitzung anzuzeigen. Ist **Farben approximieren** aktiv, wird das Farbblinken beim Umschalten von Fenstern vermieden.
Fenstergröße	Festlegen der Breite und Höhe des Fensters.
Systray Icons in Windowmanager Taskleiste einbetten	Einfügen eines Anwendungsicons in ihre lokale Taskleiste
Schriftglättung	Aktivieren der Schriftglättung - Schalten Sie die Schriftglättung bei Performanceproblemen aus, da sie zusätzliche Rechenzeit fordert.
Multi Monitor	Festlegen, ob der Vollbildmodus auf alle Monitore ausgedehnt werden soll.

5.2.4. Tastatur

Auf der Seite **Tastatur** können Sie alternative Tastenkombinationen für üblicherweise in ICA-Sitzungen verwendete Hotkeys definieren. In MS Windows wird beispielsweise mit der Tastenkombination Alt+F4 das aktuelle Fenster geschlossen. Sie funktioniert auch in ICA-Sitzungen. Alle Tastenkombinationen mit Alt, die nicht vom X Window Manager verwendet werden, funktionieren in der ICA-Session auf die bekannte Weise.

Standardmäßig werden die Tastenalternativen auf Strg+Umschalt+Taste gelegt. Sie können die Festlegungen jedoch ändern, indem Sie auf das Drop-down-Feld **Hotkeymodifikation** und/oder Hotkeyzeichen der jeweiligen Tastenkombination klicken.

- Mögliche Tasten: F1 – F12 , Plus, Minus, Tab
- Mögliche Modifier: Umschalt, Strg, Alt, Alt+Strg, Alt+Umschalt, Strg+Umschalt

> Wenn Sie die PC-Tastenkombination Strg Alt Entf während einer ICA-Sitzung nutzen möchten, verwenden Sie die Tastenkombination Strg Alt Enter oder Strg Alt Eingabetaste.

5.2.5. Mapping

Lokal angeschlossene Geräte wie Drucker oder USB-Speicher lassen sich in ICA-Sitzungen verfügbar machen.

Laufwerkszuweisung

Durch eine Laufwerkszuweisung wird jedes auf dem Thin Client eingehängte Verzeichnis (auch CD-ROMs und Diskettenlaufwerke) während ICA-Sitzungen auf Citrix-Servern für Sie verfügbar. Auf dieser Seite können Sie festlegen, welche Ordner oder Laufwerke bei der Anmeldung zugewiesen werden. Dies gilt für alle ICA-Verbindungssitzungen.

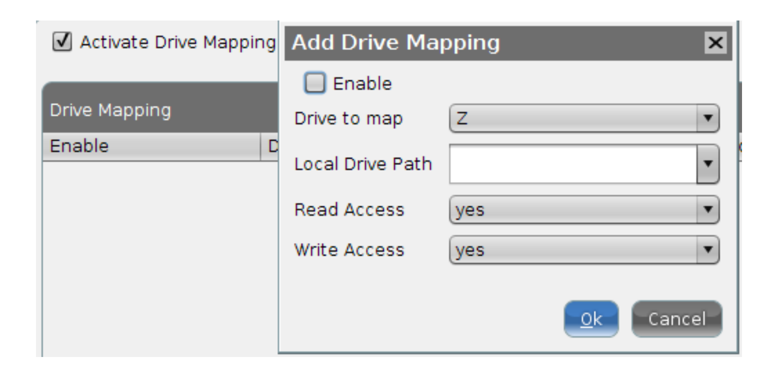


Figure 13: Laufwerkszuweisung

Die Option **Laufwerkszuweisung aktivieren** dient dazu, die Laufwerkszuweisung vorübergehend zu aktivieren/deaktivieren. Dies hat den Vorteil, dass gespeicherte Einstellungen nicht verloren gehen, jedoch ein- bzw. ausgeschaltet werden können.

> Lokale (USB-)Geräte, die für die Laufwerkszuweisung verwendet werden sollen, müssen zunächst als Gerät eingerichtet werden.

So richten Sie Laufwerkszuweisungen ein:

1. Klicken Sie **Hinzufügen**, um das Zuweisungsfenster aufzurufen.
2. Wählen Sie aus der Liste ein **Ziellaufwerk** aus, unter dem das lokale Gerät oder der Ordner zugewiesen werden soll.

   > Wenn der von Ihnen ausgewählte Laufwerksbuchstabe auf dem Citrix-Server nicht mehr verfügbar ist, wird das angegebene Verzeichnis oder lokale Laufwerk bei der Anmeldung dem nächsten freien Buchstaben zugewiesen.

3. Geben Sie den Pfadnamen des lokalen Verzeichnisses an, auf das die Zuweisung verweisen soll.

   > Wenn Sie ein lokal angeschlossenes Gerät zuweisen, verwenden Sie die im Drop-down-Feld angebotenen vordefinierten Pfadnamen. Es handelt sich dabei um die Verzeichnisse, in die die Geräte standardmäßig beim Bootvorgang eingehängt sind (z. B. /autofs/floppy für ein integriertes Diskettenlaufwerk).

4. Geben Sie die Zugangsberechtigungen für die Zuweisung an.

   Sie haben für jede Zuweisung gesondert die Möglichkeit, **Lesezugriff** oder **Schreibzugriff** zu gewähren oder können die Option **Nachfrage** wählen, dann wird beim Erstzugriff pro ICA-Sitzung nach dem Lese-/Schreibzugriff gefragt.

> Die hier definierten Laufwerkszuweisungen und Zugangsdaten sind für alle ICA-Verbindungen gültig.

COM-Ports - Serielle Anschlüsse

Aktivieren Sie **Com Port Mapping**, um eine bidirektionale Zuweisung zwischen seriellen Geräten durchzuführen, die an den Thin Client (z. B. Scanner, serielle Drucker) und den seriellen Anschlüssen des Citrix-Servers angeschlossen sind.

Auf diese Weise können die auf dem Server ausgeführten Programme Daten mit den lokalen Geräten austauschen.

- Klicken Sie Hinzufügen unter **Serielle Geräte**.
- Wählen Sie aus der Drop-down-Liste den seriellen Anschluss aus, mit dem ein Gerät verbunden ist oder klicken Sie **Geräte suchen...** um ein verfügbares Gerät auszuwählen.

/dev/ttyS0	steht für den lokalen seriellen Anschluss COM1
/dev/ttyS1	steht für den lokalen seriellen Anschluss COM2
COM3 und COM4	steht für potenzielle Ergänzungskarten, die im PCI/ISA-Steckplatz installiert sind, z. B. ein internes Modem
USB COM1 bis USB COM4	stehen für serielle Anschlüsse an USB-zu-Seriell-Adaptern.

Ihre Auswahl wird dem virtuellen COM1-Anschluss zugewiesen. Ein zweites Gerät wird dem virtuellen COM2-Anschluss zugewiesen usw.

Drucker

Richten Sie hier einen Drucker für ICA-Sitzungen ein.

Mit der Funktion **Client Drucker aktivieren** wird der lokal angeschlossene Drucker des Thin Clients für Ihre ICA-Sitzungen verfügbar gemacht, vorausgesetzt, er wurde nicht serverseitig deaktiviert.

Die Drucker müssen auf der Seite **Geräte→Drucker→CUPS→Drucker** eingerichtet sein und dort für das Mapping in ICA-Sitzungen freigegeben werden, siehe *ICA-Sitzungen* (Seite 34).

Da der Thin Client die eingehenden Druckaufträge lediglich in eine Warteschlange stellt, müssen Sie den Drucker auf dem Server installieren.

Geräteunterstützung

Aktivieren Sie virtuelle ICA-Kanäle für die Kommunikation mit verschiedenen am Thin Client angeschlossenen Geräten. Dies können z. B. Kartenleser, Diktiergeräte oder auch USB-Speicher sein. Der jeweilige Kanal ermöglicht die Kommunikation des Geräts mit der entsprechenden Serveranwendung.

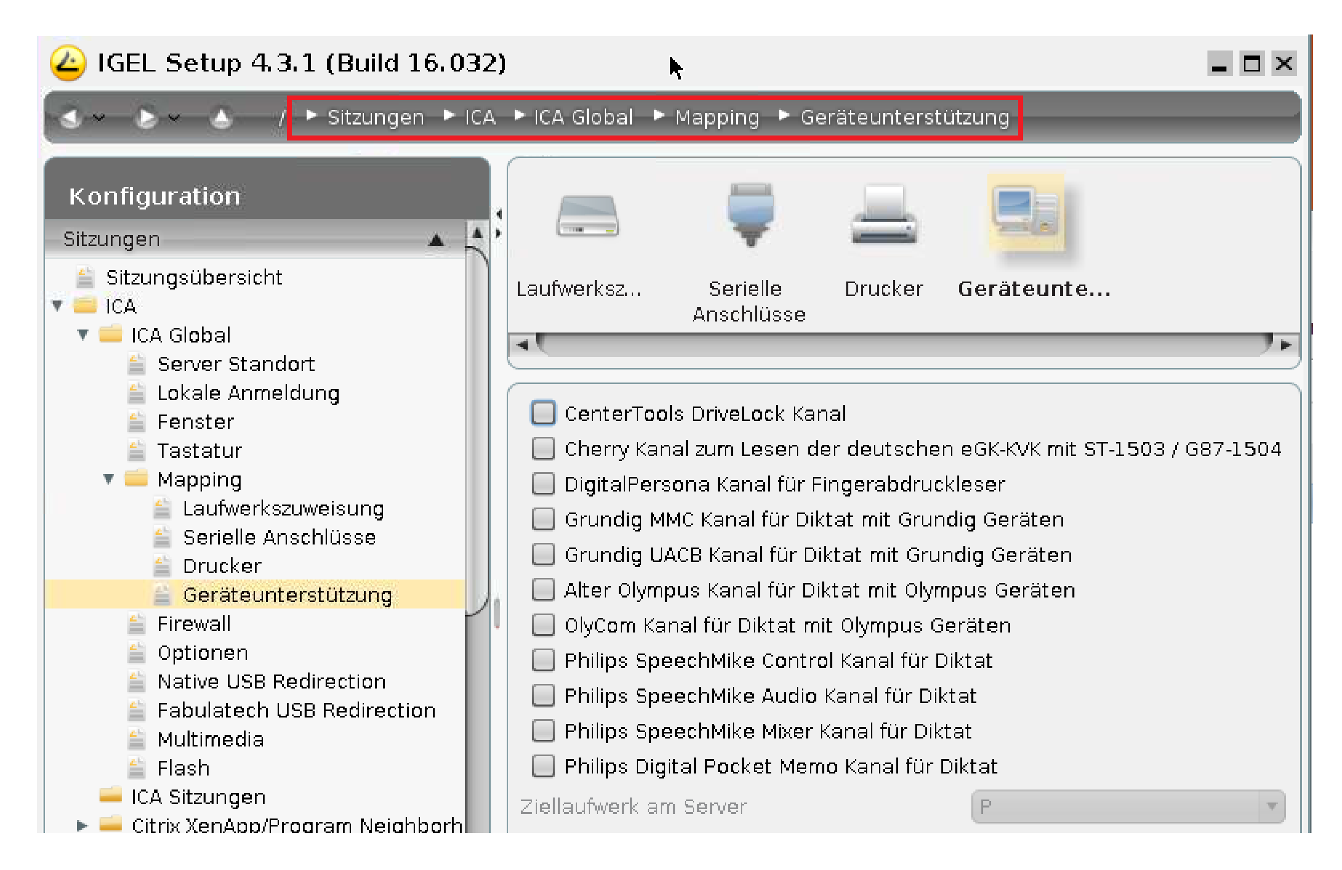


Figure 14: unterstützte Geräte

> Achten Sie beim Einsatz von CenterTools DriveLock darauf, dass die Verwendung von USB-Geräten nicht global beschränkt ist: **Geräte→USB Zugriffskontrolle**

DriveLock

Der virtuelle DriveLock-Kanal (ICA-Protokoll) ist ab Version 4.11.100 direkt im UDLX implementiert und muss auf dem Citrix-XenApp-Server installiert werden.

DriveLock kann Hardwaredaten von lokalen USB-Geräten lesen und diese mit Hilfe der Virtual ICA-Channel Extension auf den XenApp-Server übertragen. Für die Nutzung von Whitelists werden Regeln berücksichtigt, die auf Hardwareeigenschaften des verbundenen Laufwerks basieren, wie Herstellerangaben, Modell und Seriennummer.

Folgende Voraussetzungen sind wichtig, um über die DriveLock-Serverkonfiguration die Zugriffsrechte für Laufwerke festlegen zu können:

- Aktivieren Sie die USB-Geräte über die Laufwerkszuweisung, damit sie innerhalb Ihrer Terminalsitzung als Laufwerke zur Verfügung stehen.
- Überprüfen Sie die Einstellungen unter **Sitzungen→ICA→ICA Global→Mapping→Laufwerkszuweisung**, sie sollten mit den DriveLock-Einstellungen korrespondieren.

- Deaktivieren Sie Citrix-USB-Redirection, weil dies sonst die Laufwerkserkennung von DriveLock behindert.
- Überprüfen Sie die Einstellungen unter Geräte **Geräte→Speichergeräte→USB Storage Hotplug**, da sie Einfluss auf die USB-Geräte in der Citrix-Sitzung haben können.
- Installieren und aktivieren Sie den DriveLock-Kanal im Universal Desktop-Setup unter **Sitzungen→ICA→ICA Global→Mapping→Geräteunterstützung**.

Im Downloadbereich von Centertools finden Sie ein Dokument, welches die Konfiguration von DriveLock auf der Serverseite genauer beschreibt: How to use Centertools DriveLock with IGEL Thin Clients

DigitalPersona Authentifikation

Mit der Integration von DigitalPersona Fingerabdrucklesern im System des Thin Clients und der dazugehörigen serverseitigen Software können sich Nutzer von IGEL Thin Clients auch per Fingerabdruck an virtuellen Anwendungen auf einem Citrix XenApp-Server identifizieren. Alle x86-basierten IGEL Thin Clients mit IGEL Linux Betriebssystem unterstützen das Handling der Anmeldedaten über die DigitalPersona Pro Enterprise Software (Version v5.3 und v5.4).

In Verbindung mit den DigitalPersona U.are.U 4500 Fingerabdrucklesern, die per USB an die IGEL Thin Clients angeschlossen werden, wird eine sichere und schnelle Form der Authentifizierung auf virtuelle Desktops gewährleistet.

Aktivieren Sie den entsprechenden virtuellen Kanal in der **Geräteunterstützung**, um den Fingerabdruckleser in Citrix Sitzungen verwenden zu können.

Softpro SPVC Kanal

- Aktivieren Sie den **Softpro SPVC Kanal für Signaturtablets**, um Softpro/Kofax Tablets in Citrix-Citzungen zu verwenden.

  Detaillierte Hinweise zur Konfiguration von Signaturpads finden Sie in Best Practices zu StepOver Pads und SoftproSoftpro/Kofax Pads.

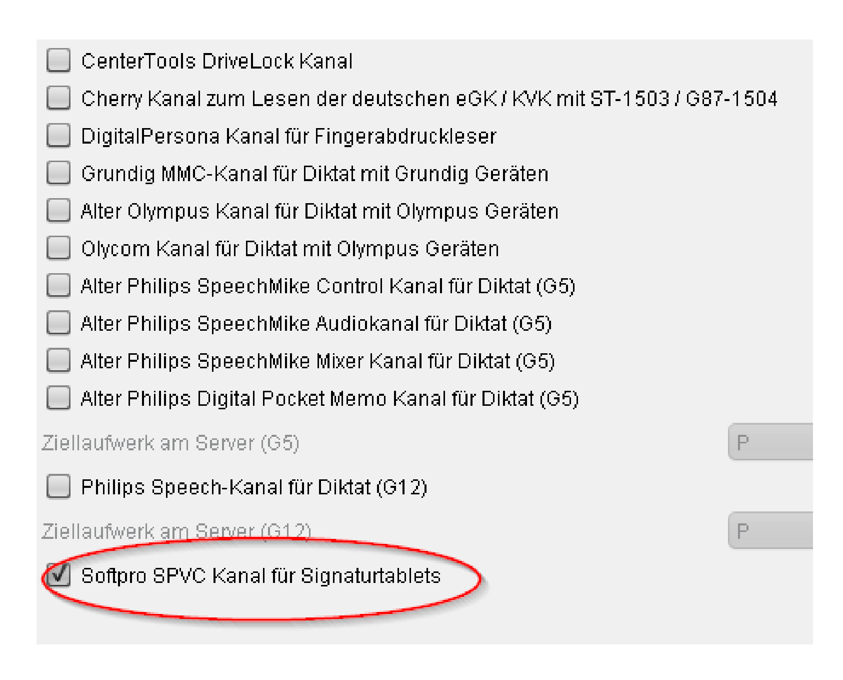


Figure 15: Softpro SPVC Kanal

5.2.6. Firewall

Alternative Adresse verwenden	Definieren Sie einen Proxy oder Secure Gateway Server als alternative Adresse bei Verbindungen über eine Firewall. Beachten Sie die Tooltips zu den einzelnen Parametern der Konfiguration.
SOCKS / Sicherer Proxy	Wählen Sie hier die Standardproxyeinstellungen aus oder definieren Sie selbst welche.
Proxytyp	Verwenden Sie Secure (HTTPS), so muss SSL/TLS oder 128-bit-Verschlüsselung aktiviert sein, damit eine sichere Verbindung aufgebaut werden kann.
Secure Gateway (relay mode)	Wenn Sie ein Citrix Secure Gateway im Relay-Modus verwenden wollen, müssen Sie den vollen Domainnamen angeben - die IP-Adresse genügt in diesem Fall nicht.

> Fügen Sie nach der Aktivierung der Alternativadresse den Server in **Globale Einstellungen für ICA** im Feld **Serverstandort** zur Adressliste hinzu.

5.2.7. Optionen ICA Global

Auf dieser Seite können Sie zusätzliche Optionen einrichten, um das allgemeine Verhalten und die Leistung zu optimieren.

Server Redraw verwenden	Der Citrix-Server kontrolliert das Auffrischen des Bildschirminhalts.
Windows Warntöne deaktivieren	Durch diese Option werden die Windows-Warntöne deaktiviert.
Backing Store verwenden	Der X-Server speichert temporär verdeckte Arbeitsflächenfensterinhalte.
Verzögerter Bildschirmupdatemodus	Aktiviert verzögerte Aktualisierungen vom lokalen Videopuffer auf dem Bildschirm. Der lokale Videopuffer wird verwendet, wenn der Seamless-Windows-Modus oder HDX-Latenz-Reduktion verwendet werden.
Größe des Zwischenspeichers in kB	Verändern der Einstellung für den Bitmapzwischenspeicher (Cache). Wenn Sie mit Bildern arbeiten, die immer wieder angezeigt werden, können Sie die Leistung Ihrer ICA-Sitzung(en) erheblich verbessern. Legen Sie die maximale Größe des für das Zwischenspeichern genutzten lokalen Systemspeichers (in Kilobyte) fest. Bestimmen Sie außerdem die Mindestgröße der Bitmapdateien, die im Zwischenspeicher gespeichert werden sollen sowie das Verzeichnis, in dem die Dateien lokal abgelegt werden sollen.

Eine zu hohe Einstellung kann bewirken, dass der Thin Client über zu wenig Speicher für das eigene System und andere Anwendungen verfügt. Sie haben im Zweifelsfall die Möglichkeit, Ihren Thin Client mit zusätzlichem RAM auszustatten.

Bildlaufkontrolle	Je nach Geschwindigkeit Ihres Netzwerks oder der Antwortzeit Ihres Servers, kann es (z. B. in EXCEL) zu einer Verzögerung zwischen dem Loslassen der Maustaste auf einer Bildlaufleiste und dem Anhalten des Bildlaufvorgangs kommen. Dieses Problem kann möglicherweise behoben werden, indem Sie den Wert auf 100 oder höher setzen.
Automatische Wiederverbindung aktivieren	Festlegen der Parameter für die Wiederverbindung der Sitzung
Kerberos Passthrough-Authentifizierung in Program Neighborhood Sitzungen erlauben	Ermöglicht die Verwendung von Kerberos Pass-Through-Authentifizierung in der Citrix Program Neighborhood Sitzung.

5.2.8. USB-Redirection

USB-Geräte können anhand von Regeln in einer Citrix-Sitzung zugelassen oder verboten werden, dabei sind auch Unterregeln für Geräte oder Geräteklassen möglich. Die Verwendung der Regeln ist beschrieben unter *USB-Zugriffskontrolle* (Seite 112).

Verwenden Sie entweder die **Native USB-Redirection** oder die **Fabulatech USB-Redirection**.

Für **Fabulatech USB-Redirection** muss auf dem Citrix Server eine spezielle Fabulatech Serverkomponente installiert werden (USB for Remote Desktop Igel Edition).

Nähere Informationen zur Funktion finden Sie auf der Fabulatech-Partnerseite: *http://www.usb-over-network.com/partners/igel/ http://www.usb-over-network.com/partners/igel/*.

> Aktivieren Sie entweder die native oder die Fabulatech USB-Redirection – nicht beide zusammen.
>
> Deaktivieren Sie die USB-Redirection, falls Sie Centertools DriveLock (Seite 29) verwenden.

5.2.9. HDX Multimedia Redirection

Citrix-HDX-Multimediabeschleunigung verbessert die Wiedergabe über Media Player innerhalb einer ICA-Sitzung auf dem Remote Desktop und ermöglicht die Verwendung isosynchroner Übertragungen z.B. von Webcams innerhalb der Sitzung.

Siehe Unterstützte Formate und Codecs.

Aktiviere Multimedia Redirection
HDX Realtime WebCam Redirection
HDX WebCam Framerate 5
Bildqualität der HDX WebCam 16
Bildbreite der HDX WebCam 352
Bildhöhe der HDX WebCam 288
HDX WebCam Verzögerungszeit 2000
HDX WebCam Verzögerungstyp 1
HDX Realtime Media Engine verwenden
Inhaltsumleitung aktivieren

Figure 16: Multimedia Redirection

So verbessern Sie die Multimediawiedergabe auf dem Remote Desktop:

1. Stellen Sie sicher, dass die benötigten Codecs auf der Remote-Desktopseite installiert sind, um die verbesserte Wiedergabe zu nutzen.
2. Aktivieren Sie die Multimedia-Redirection auf dem Thin Client.
3. Erstellen Sie die Sitzung.
4. Starten Sie die Wiedergabe auf dem entfernten Desktop.

> Ab IGEL Linux 5.06.100 ist auf bestimmten Geräten Hardwarebeschleunigung für Multimedia-Wiedergabe verfügbar. Näheres entnehmen Sie einem FAQ-Dokument zum Thema.

5.2.10. Flash

Die Citrix HDX Mediastream Redirection für Flash erlaubt je nach Leistungsfähigkeit des Thin Clients eine flüssigere Darstellung von Flash-Inhalten als bei der Wiedergabe innerhalb der Citrix-Sitzung selbst.

> Die Aktivierung der Flash-Umleitung setzt ein installiertes Flashplayer Browser Plugin voraus. Installieren Sie das Plugin unter **Sitzungen→Browser→Plugins→Flashplayer.**

5.2.11. Codec

Für die Citrix-Versionen 13.x stehen zwei Codecs für die Wiedergabe der Bildschirminhalte zur Auswahl:

- Die Standardeinstellung **Automatisch** wählt automatisch den für die Leistungsfähigkeit der Hardware geeigneten Codec aus.
- Alternativ lassen sich die Codecs **H.264** (für hohe Qualität komplexer Grafikinhalte) und **JPEG** (weniger CPU-intensiv) sowie ihre Optionen auch von Hand auswählen.

> Ist Version 12.x des Citrix-Receivers ausgewählt, ist diese Setupseite nicht bearbeitbar.

5.3. Citrix ICA-Sitzungen

Wenn eine Sitzung erstellt oder bearbeitet wird können Sie die ICA-Sitzungseinstellungen ändern, sofern sie sich von den globalen Einstellungen unterscheiden.

> Die erste Quelle für weitere Informationen zu Citrix-Verbindungen sollte immer die entsprechende Dokumentation von Citrix sein. In diesem Handbuch werden lediglich allgemeine Konfigurationshinweise gegeben.

5.3.1. Server

Browserprotokoll	Auswählen des für die Übertragung benötigten Protokolls oder der globalen Standardeinstellung
Standardserverstandort nicht verwenden	Aufhebung der Standardservervorgabe - für jedes Protokoll gesondert
Server	Durch Klicken auf die Schaltfläche **Suche** senden Sie ein Übertragungssignal, das alle verfügbaren Server und veröffentlichten Anwendungen anfragt. • Durch Auswählen des Servers wird der Benutzer mit der kompletten Arbeitsfläche verbunden, als würde er sich vor dem Server selbst anmelden. Damit stehen alle in seinem Benutzerprofil (lokales Serverprofil) angegebenen Anwendungen, Rechte und Einstellungen zur Verfügung. • Wird eine der veröffentlichten Anwendungen ausgewählt, wird die Sitzung in einem Fenster geöffnet, das nur eine Anwendung enthält. Die Sitzung wird beendet, wenn Sie diese Anwendung schließen. • Sie können die IP-Adresse oder den Hostnamen des Servers auch manuell in das Feld **Server** eingeben.
Applikation	Wenn Sie den Server manuell eingetragen haben, können Sie hier eine veröffentlichte Anwendung angeben. Diese Felder werden automatisch ausgefüllt, wenn Sie eine der erkannten veröffentlichten Anwendungen ausgewählt haben.
Arbeitsverzeichnis	Angabe des Pfadnamens des Arbeitsverzeichnisses für die Anwendung

5.3.2. Anmeldung

Kerberos Passthrough-Authentifizierung verwenden	Aktivierung von Single Sign-on für diese ICA-Sitzung, falls die Anmeldung am Thin Client mit AD/Kerberos konfiguriert ist. Auch der Server muss für Passthrough-Authentifizierung konfiguriert sein. Beim Start der ICA-Sitzung ist dann keine erneute Benutzername- und Passworteingabe erforderlich.
Passthrough-Authentifizierung verwenden	Aktivierung von Single Sign-on für diese ICA-Sitzung, falls die Anmeldung am Thin Client mit AD/Kerberos konfiguriert ist. Durch Zwischenspeichern von Benutzername und Passwort bei der Anmeldung am Thin Client ist beim Sitzungsstart keine erneute Eingabe erforderlich.
Benutzer, Passwort, Domäne	Hier können Benutzername, Passwort und Domäne für die ICA-Sitzung eingegeben werden. Diese Angaben werden automatisch an den Server weitergeleitet und müssen auf dem Anmeldebildschirm nicht mehr eingegeben werden.
Passwortschutzfenster vor Anmeldung nicht anzeigen	Die Option schaltet den Windows-Eingangsbildschirm ein und aus. Für die Windows-Anmeldung mit Smartcard muss diese Option deaktiviert werden.

5.3.3. Fenster

Unter **Fenstereinstellungen** nehmen Sie folgende Konfigurationen vor:

Anzahl an Farben	Die Farbtiefe ist als **globaler Standard** festgelegt. Sie können sie für diese Sitzung ändern.
Standardeinstellungen für Farbtabelle verwenden	Die Farbtabelle ist global voreingestellt. Sie können sie für diese Sitzung **approximieren**.
Vollbildmodus	Durch Deaktivieren des **Vollbildmodus**, kann man zwischen der globalen Standardeinstellung und einer sitzungsspezifischen Einstellung wählen.
Startmonitor	Festlegen, welcher Bildschirm in einer Umgebung mit mehreren Monitoren für die Sitzung verwendet werden soll.
Seamless Window Modus aktivieren	Der Seamless Window-Modus kann nur mit veröffentlichten Anwendungen oder mit einem festgelegten Startprogramm für die Serververbindung genutzt werden.
Schriftglättung	Die Schriftglättung ist global voreingestellt. Sie können sie für diese Sitzung ändern.

5.3.4. Firewall

Alternative Adresse verwenden	Definieren Sie einen Proxy oder Secure Gateway Server als alternative Adresse bei Verbindungen über eine Firewall. Beachten Sie die Tooltips zu den einzelnen Parametern der Konfiguration.
SOCKS / Sicherer Proxy	Wählen Sie hier die Standardproxyeinstellungen aus oder definieren Sie selbst welche.
Proxytyp	Verwenden Sie Secure (HTTPS), so muss SSL/TLS oder 128-bit-Verschlüsselung aktiviert sein, damit eine sichere Verbindung aufgebaut werden kann.
Secure Gateway (relay mode)	Wenn Sie ein Citrix Secure Gateway im Relay-Modus verwenden wollen, müssen Sie den vollen Domainnamen angeben - die IP-Adresse genügt in diesem Fall nicht.

Fügen Sie nach der Aktivierung der Alternativadresse den Server in **Globale Einstellungen für ICA** im Feld **Serverstandort** zur Adressliste hinzu.

5.3.5. Wiederverbindung

- Aktivieren Sie **Standardeinstellungen zur automatischen Wiedererkennung verwenden**, um die unter **HDX / ICA Global** > **Wiederverbindung** vorgenommenen Einstellungen zu übernehmen.
- Alternative aktivieren Sie die **Automatische Wiederverbindung** und haben hier die Möglichkeit, die Anzahl der maximalen Versuche und die zeitliche Verzögerung vor einer Wiederverbindung anzugeben.

5.3.6. Optionen

Optimieren Sie unter **Optionen** die Leistung und das Verhalten innerhalb der ICA-Sitzung.

Komprimierung	Verringern der Datenmenge, die über die ICA-Sitzung übertragen wird - Dadurch wird der Netzwerkverkehr zu Lasten der CPU-Leistung reduziert. Wenn Sie Ihre/n Server per WAN verbinden, sollten Sie die Komprimierung nutzen. Wenn Sie einen leistungsschwächeren Server verwenden und Sie nur in einem LAN arbeiten, deaktivieren Sie diese Option.
Zwischenspeicherung von Bilddaten	Aktiviert für jede Sitzung die Zwischenspeicherung im Cachespeicher (konfiguriert in den globalen ICA-Einstellungen) - Dies ist dann sinnvoll, wenn Sie mehrere ICA-Sitzungen nutzen, jedoch nur eine oder zwei Sitzungen kritisch im Hinblick auf die Netzwerkbandbreite sind oder während des Tages stark genutzt werden. In diesem Fall sollten Sie den Cachespeicher für diese Sitzungen reservieren.
Verschlüsselungsmethode	Durch die Verschlüsselung wird die Sicherheit Ihrer ICA-Verbindung erhöht. Standardmäßig ist die Basisverschlüsselung aktiviert. Vergewissern Sie sich deshalb, dass der Citrix-Server die RC5-Verschlüsselung unterstützt, bevor Sie einen höheren Verschlüsselungsgrad wählen.
Audioübertragung	Übertragen der Systemtöne und Audioausgaben von den Anwendungen auf den Thin Client - Über die angeschlossenen Lautsprecher werden sie gesendet. Je höher die von Ihnen gewählte Audioqualität ist, umso mehr Bandbreite wird für die Übertragung der Audiodaten benötigt.
Mausklick Feedback	Visuelle Rückmeldung auf einen Mausklick, indem sich der Mauszeiger umgehend in ein Sanduhrsymbol ändert.
Lokales Textecho	Schnellere Anzeige des Eingabetextes und Vermeidung von Latenzen im Netzwerk - Wählen Sie einen Modus aus der Drop-down-Liste aus: • Wählen Sie **Ein** für langsamere Verbindungen (Verbindung über ein WAN), um die Verzögerung zwischen Benutzereingabe und Anzeige auf dem Bildschirm zu verringern. • Setzen Sie den Modus für schnellere Verbindungen (Verbindung über ein LAN) auf **Aus**. • Wählen Sie den Modus **Automatisch**, wenn Sie nicht sicher sind, wie schnell die Verbindung ist.

5.3.7. Desktopintegration

- Geben Sie den **Namen** der Sitzung an, für die Sie die Integration auf dem Desktop vornehmen möchten.
- Wählen Sie aus den **Startmöglichkeiten**, wie Sie die Sitzung zugänglich machen möchten.
- Legen Sie optional einen **Hotkey** für den Start der Sitzung fest.
- Aktivieren Sie **Autostart**, um diese Sitzung direkt nach Systemstart zu starten. Geben Sie in Sekunden an, wie lange der Sitzungsstart beim Autostart verzögert werden soll.
- Aktivieren Sie **Neustart**, um die Sitzung nach Verbindungsabbau neu zu starten.

5.4. Citrix StoreFront / Web Interface

Die meisten Einstellungen wurden bereits unter HDX ICA Global und im *ICA-Sitzungssetup* (Seite 34) vorgenommen.

- Wählen Sie die Startmöglichkeiten für die Citrix XenApp-Sitzung aus, siehe **Desktopintegration**.

5.4.1. Verbindungen

- Legen Sie unter **Server Standort** die Master Browser fest, in denen veröffentlichte Anwendungen gesucht werden können.

> Sie können bis zu 5 Citrix Master Browser pro Domäne einrichten. Wenn der erste Browser nicht erreichbar ist, wird der zweite abgefragt usw. Bitte beachten Sie, dass das Durchsuchen von mehreren Farmen unterstützt wird. Deshalb können Sie Adressen für mehrere Serverfarmen festlegen.

- Klicken Sie **Citrix XenApp Serviceseite benutzen**, um Einstellungen vom Server zu holen und veröffentlichte Anwendungen über die Citrix XenApp Serviceseite zu konfigurieren

5.4.2. Optionen

Legen Sie Audio-, Tastatur- und Darstellungsoptionen fest, wenn sie sich von den globalen Einstellungen unterscheiden.

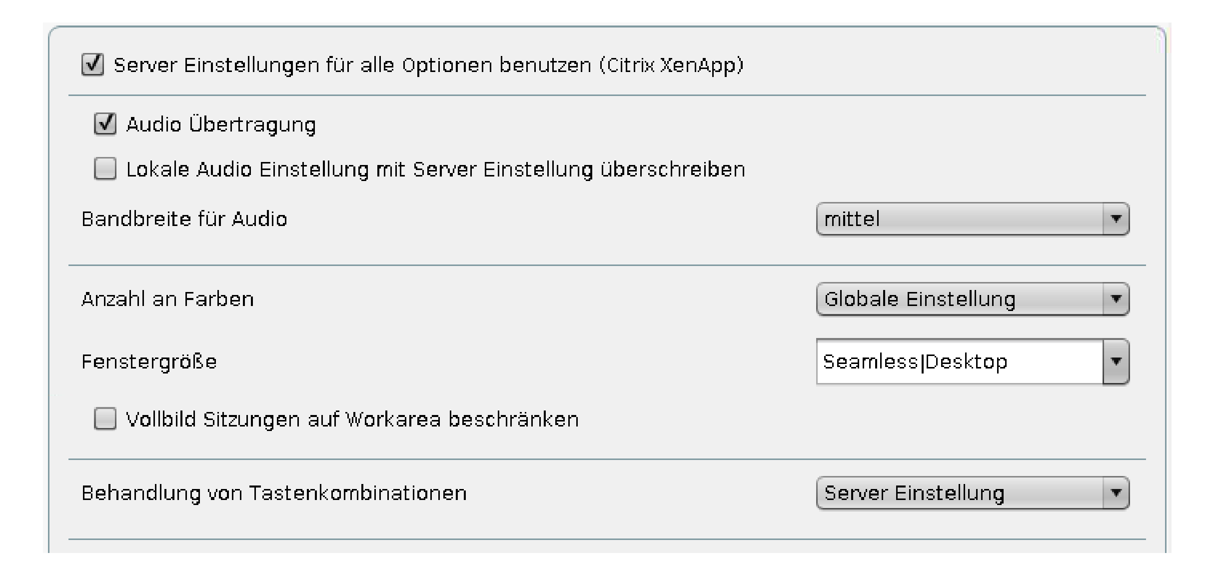


Figure 17: Optionale Einstellungen

5.4.3. Anmeldung

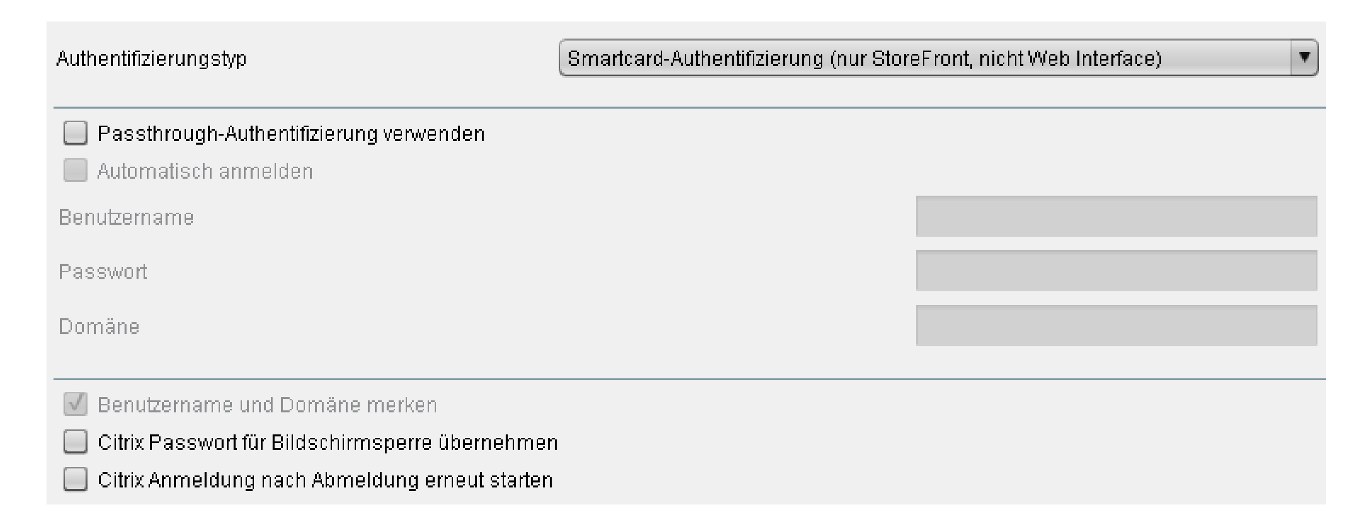


Figure 18: Citrix XenApp Anmeldung

➢ Wählen Sie einen **Authentifizierungstyp** (nicht alle Typen stehen bei allen Receiver-Versionen zur Auswahl):

- **Passwort-Authentifizierung**
- **Kerberos Pass-Through-Authentifizierung (nur Web Interface, nicht StoreFront),** verwendet lokale Logindaten für das Auflisten und Starten von Applikationen zu verwenden. Die Option aktiviert Single Sign-on für XenApp, falls die Anmeldung am Thin Client mit AD/Kerberos konfiguriert ist.
- **Smartcard-Authentifizierung (nur StoreFront, nicht Webinterface)**
- **Citrix-Autentifizierungsmechanismus (statt IGEL), ohne Smartcard**
- **Citrix-Autentifizierungsmechanismus (statt IGEL), mit Smartcard**

Haben Sie einen Typ mit Smartcard eingestellt, wählen Sie auf der Seite **Smartcard** den Typ der Karte.

Weitere Optionen:

Passthrough-Authentifizierung verwenden	verwendet zwischengespeicherte Anmeldedaten für das Auflisten und Starten von Applikationen.
Automatisch anmelden	verwendet die auf dieser Seite voreingestellten Anmeldedaten beim Verbinden mit dem Server
Citrix Passwort für Bildschirmsperre übernehmen	Synchronisiert das Passwort der Bildschirmsperre mit dem der Citrix-Anwendung
Citrix Anmeldung nach Abmeldung erneut starten	Zeigt Dialog **Anmelden** nach der Abmeldung automatisch wieder an.

Smartcard

Ab IGEL Linux 5.06.100 ist es mit Version 13.1.3 von Citrix Receiver möglich, sich per Smartcard an Citrix StoreFront anzumelden. Hier lässt sich ein Typ von **Smartcard** auswählen oder ein eigenes **PKCS#11-Modul** einbinden.

5.4.4. Erscheinungsbild

Sie können die XenApp/Program Neighborhood-Anwendungen so konfigurieren, dass sie in verschiedenen Bereichen des lokalen Systems angezeigt werden, zum Beispiel auf der lokalen Arbeitsfläche oder im Startmenü.

- Aktivieren Sie **Symbole für das Startmenü skalieren**, um die Größe des Anwendungssymbols automatisch anzupassen.

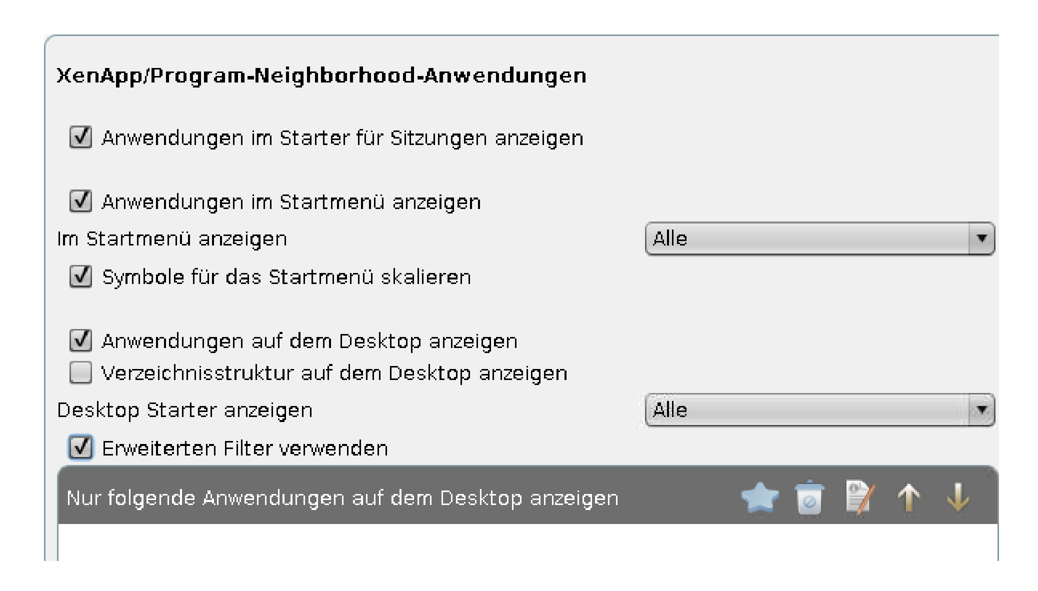


Figure 19: Citrix XenApp Layout

5.4.5. Passwortänderung

Legen Sie hier fest, wie eine Verbindung für die Passwortänderung hergestellt wird.

Generische Sitzung	Suche nach Servern und Anwendungen mit anschließendem Verbindungsaufbau
Vorkonfigurierte ICA-Sitzung	Wahl einer vordefinierte ICA-Sitzung nach Sitzungsnamen
Citrix XenApp Services-Site	Passwortänderung direkt über das Citrix-Webinterface
Kerberos zum Ändern des Passworts Benutzen	Ist Kerberos Authentifizierung am XenApp-Server eingerichtet, kann das Passwort auch darüber geändert werden.

5.4.6. Wiederverbinden und Aktualisieren

- Wählen Sie die erforderliche Option für das Wiederverbinden mit Sitzungen.

Sie können die Verbindung

- während des Anmeldevorgangs und
- durch die Nutzung einer Wiederverbindensitzung, z. B. auf dem Desktop, aufbauen.

Mit dem Wiederverbindungsverfahren können Sie **aktive und getrennte Sitzungen**, nur **getrennte Sitzungen** oder Sitzungen per **Nachfrage** starten.

Eine Aktualisierungssitzung lädt die XenApp-Sitzung neu, ohne sie zu trennen.

5.4.7. Abmelden

Ist die Option **Benutze Hotkey** aktiviert, können Sie sich von einer Sitzung per Tastenkombination abmelden. Die Kombination besteht aus **Modifier**-Tasten wie Ctrl (Steuerung), Alt und Shift (Hochstelltasten) und einer Zahl oder einem Buchstaben als **Hotkey**.

5.4.8. Desktopintegration

- Geben Sie den **Namen** der Sitzung an, für die Sie die Integration auf dem Desktop vornehmen möchten.
- Wählen Sie aus den **Startmöglichkeiten**, wie Sie die Sitzung zugänglich machen möchten.
- Legen Sie optional einen **Hotkey** für den Start der Sitzung fest.
- Aktivieren Sie **Autostart**, um diese Sitzung direkt nach Systemstart zu starten. Geben Sie in Sekunden an, wie lange der Sitzungsstart beim Autostart verzögert werden soll.

5.5. Citrix Access Gateway

Mit dem **Citrix Access Gateway** (CAG)-Client kann eine VPN-Verbindung zu einem CAG-Standardserver aufgebaut werden. Die VPN-Verbindung ist ein SSL-Tunnel. Dabei wird vom Server zum Client ein Zertifikat übertragen. Wenn das Zertifikat nicht vertrauenswürdig ist, wird eine Warnung beim Verbindungsversuch herausgegeben. Um die Warnung zu vermeiden, kann man das Serverzertifikat auf dem Thin Client in der Datei `/wfs/cagvpn/cagvpn-trusted-CAs.crt` ablegen. Außerdem kann die Warnung auch in der Konfiguration des CAG-Clients unterdrückt werden.

5.6. Appliance-Modus

Der **Appliance-Modus** kann für folgende Sitzungstypen aktiviert werden (sofern sie auf dem System zur Verfügung stehen):

- VMware Horizon
- Citrix XenDesktop
- RHEV/Spice
- Imprivata
- RDP Multipoint Server

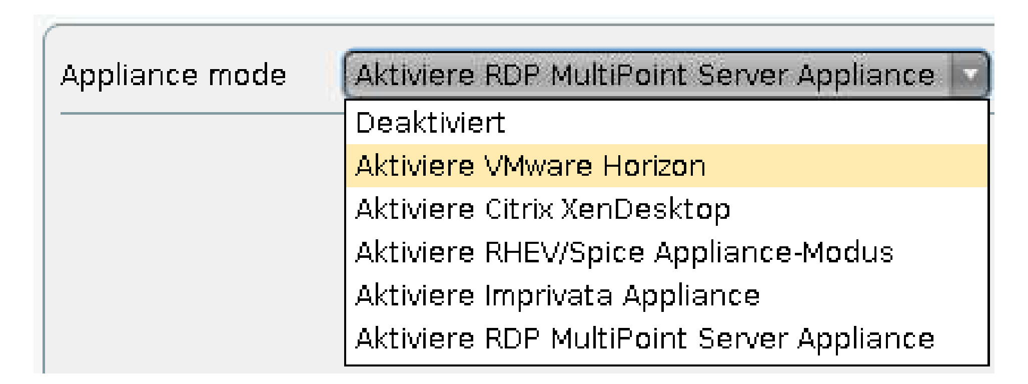


Figure 20: Sitzungstypen für den Appliance-Modus

Wenn Sie einen Appliancemodus ausführen, ist kein anderer Anwendungszugriff möglich. Nur die Serversitzung für den festgelegten Virtualisierungsserver wird angezeigt.

> Der Systemhotkey Strg+Alt+s zum Starten der IGEL Setupanwendung funktioniert im Appliance-Modus nicht. Bitte verwenden Sie stattdessen Strg+Alt+F2.

1. Aktivieren Sie eine der Appliance-Optionen.
2. Weitere Konfiguration:
   - Für VMWare Horizon, Citrix XenDesktop und RHEV/Spice:

     Konfigurieren Sie den Zugang zum entsprechenden Server also zum VMware-Horizon-Server, XenDesktop-Delivery-Server oderRHEV/Spice auf der gegenwärtigen Setupseite sowie in den globalen Einstellungen der jeweiligen Sitzungsart.
   - Für Imprivata:

     Konfigurieren Sie **URL des Servers**, **Pfad zu der Anwendung** und weitere Einstellungen direkt auf der gegenwärtigen Setupseite.

- Für RDP Multipoint Server:

  Einen oder mehrere RDP Multipoint-Server findet IGEL Linux selbstständig, wenn sich diese im selben Netzwerk befinden. Zudem müssen diese ihre IP-Adresse vom selben DHCP-Server beziehen wie der Thin Client. Im Appliance-Modus sehen Sie dann eine Auswahlliste mit Servern, mit denen Sie sich verbinden können:

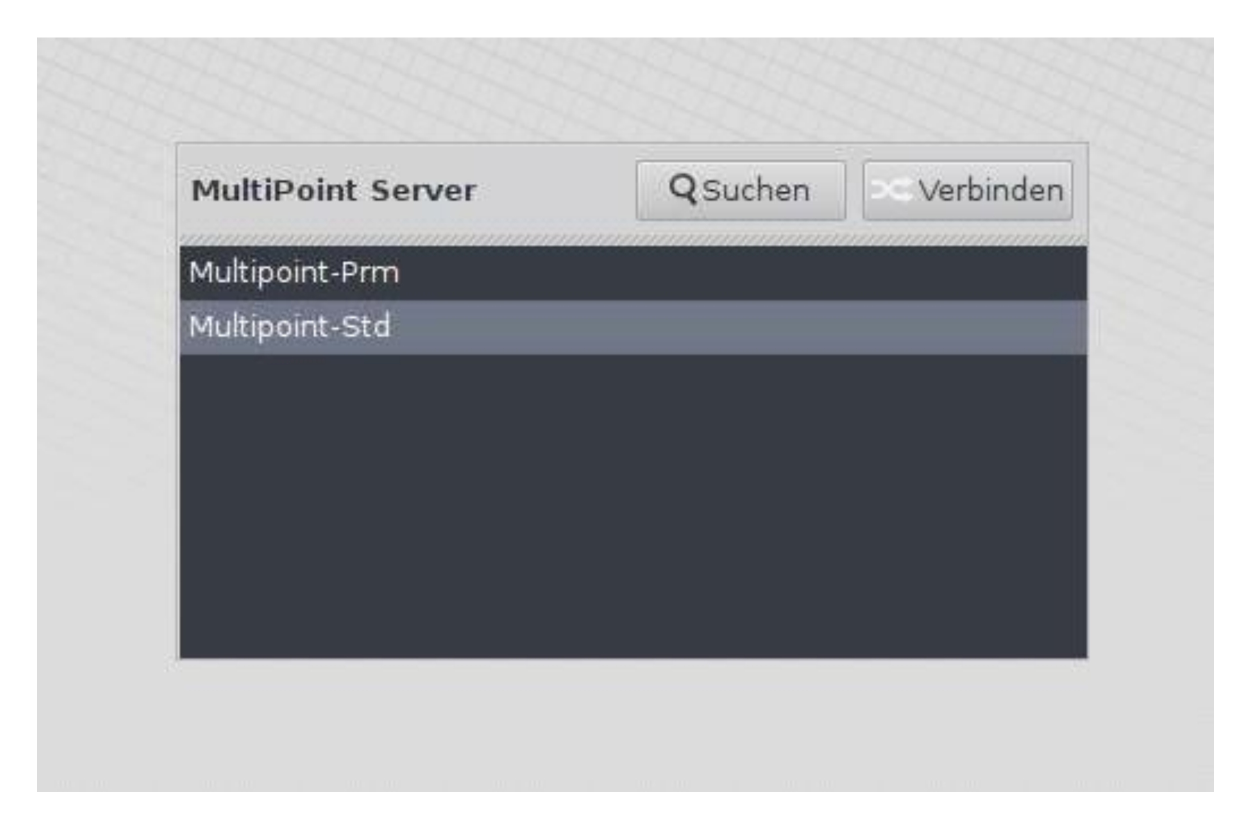


Figure 21: Auswahlliste der RDP Multipoint Server

5.7. SSH-Sitzung

In diesem Abschnitt wird beschrieben, wie Sie eine SSH Session (SSH-Sitzung) konfigurieren.

Verwenden Sie die SSH-Sitzung, um eine Remote-Anwendung über SSH (Secure Shell) auf einem Host zu starten und auf dem Terminal anzuzeigen. SSH ermöglicht die sichere verschlüsselte Kommunikation über ein unsicheres Netzwerk zwischen zwei Hosts, oder Host und Terminal . X11-Verbindungen können ebenfalls über diesen sicheren Kanal geleitet werden.

Kommando		Alle erforderlichen Einträge für die Erstellung eines ausführbaren Befehls zum Fernstart der Anwendung über SSH
	Benutzername (remote)	Name des Remote-Benutzers - Der gewählte Benutzer muss über ein Benutzerkonto auf dem Remote-Host verfügen.
	Rechner (remote)	Name oder IP-Adresse des Remote-Hosts, von dem die Remote-Anwendung gestartet wird.
	Kommandozeile	Eingabe des Namens des Anwendungsprogramms, das gestartet werden soll.

Optionen

X11-Verbindung weiterleiten	X11-Verbindungen werden automatisch an den Remote-Computer weitergeleitet, sodass jedes aus der Shell, oder dem Befehl, gestartete X11-Programm den verschlüsselten SSH-Kanal durchläuft. Die Authentifizierungsdaten werden auch automatisch festgelegt. Diese Option ist standardmäßig aktiviert.
Kompression aktivieren	Verringern der Menge der über den Datenkanal übertragenen Daten - Diese Option ist standardmäßig deaktiviert.
Protokollversion erzwingen	Sie müssen Ihre Identität gegenüber dem Remote-Host durch eine der verschiedenen Identifizierungsmethoden nachweisen. Diese hängen von der verwendeten Protokollversion ab. In diesem Bereich können Sie die Protokollversion erzwingen, nachdem Sie sich für eine Identifizierungsmethode entschieden haben.

Detaillierte Informationen zu SSH und den verschiedenen Authentifizierungsmethoden finden Sie auf den entsprechenden Handbuchseiten Ihres Serverbetriebssystems.

5.8. Firefox Browser

Die originalen Konfigurationsparameter des Webbrowsers Firefox 38.1.0 ESR werden dem IGEL Setup zugewiesen, um die zentrale Konfiguration über die IGEL UMS zu ermöglichen. Diese globalen Einstellungen können für jede Browsersitzung geändert werden.

5.8.1. Browser Global

In diesem Bereich bestimmen Sie die Startseite des Browsers, die Bildschirmauflösung und Schriftgröße.

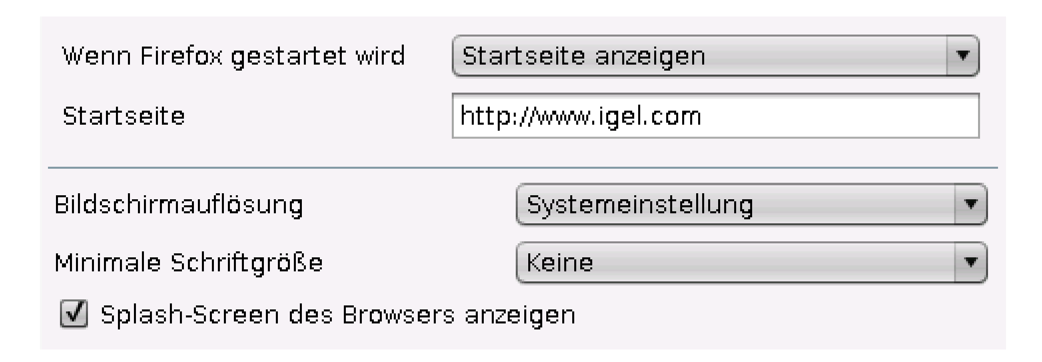


Figure 22: Einstellungen unter Browser Global

- Wählen Sie unter folgenden Optionen den für Sie passenden Startbildschirm:
  - **Leere Seite anzeigen**
  - **Startseite anzeigen**
  - **Mit letzter Seite fortsetzen**
  - **Vorherige Sitzung wiederherstellen**
- Geben Sie unter **Startseite** die URL an, wenn Sie Firefox mit der Startseite beginnen möchten.
- Wählen Sie die gewünschte **Bildschirmauflösung** in DPI - z. B. 72 für mittelgroße Bildschirme, 96 für große Bildschirme.
- Geben Sie optional eine **Minimale Schriftgröße** an.
- Deaktivieren Sie bei Bedarf den **Splash Screen des Browsers**, standardmäßig ist er aktiviert.

Tabs

In diesem Bereich bestimmen Sie die Einstellungen, die die einzelnen Tabs im Browser betreffen.

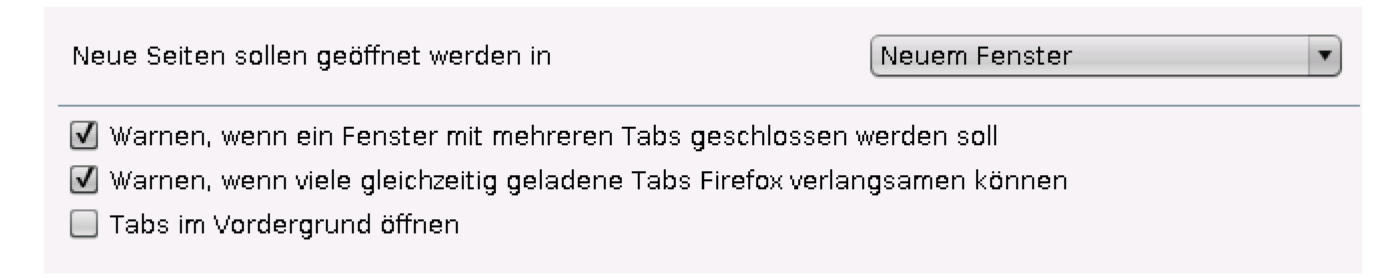


Figure 23: Tabs-Einstellungen

➢ Wählen Sie aus, ob eine neue **Browserseite** im aktuellen Browserfenster, in einem neuen Browserfenster oder in einem neuen Tab geöffnet werden soll.

Standardmäßig werden Sie gewarnt, wenn sie mehrere Tabs gleichzeitig schließen und wenn zu viele Tabs geöffnet sind und sich dadurch die Browserleistung verlangsamt.

➢ Deaktivieren Sie die jeweiligen Kontrollkästchen, um die Warnungen auszuschalten.

Standardmäßig ist eingestellt, dass Tabs, die von Links geöffnet werden, im Vordergrund öffnen.

➢ Deaktivieren Sie das Kontrollkästchen **Tabs im Vordergrund öffnen**, um diese Tabs im Hintergrund zu laden.

Inhalt

In diesem Bereich definieren Sie alle Einstellungen, die Popupfenster und Downloads betreffen.

Popup blockieren Ausnahmen...
Bilder automatisch laden Ausnahmen...
Art des Downloadverzeichnisses Benutzerdefinierter Pfad
Downloadpfad /tmp
JavaScript aktivieren
Existierende Fenster verschieben oder deren Größe ändern
Fenster vor oder hinter andere Fenster legen
Statusleiste ausblenden
Text der Statusleiste verändern
Kontextmenü verändern oder ersetzen
Sprachen für Webseiten en, de, it, fr

Figure 24: Einstellungen zum Browserinhalt

Popup blockieren ist standardmäßig aktiviert.

- Deaktivieren Sie das Kontrollkästchen, um Popups beim Laden von Seiten zuzulassen.
- Bestimmen Sie **Ausnahmen**, um bestimmte Popups von der gewählten Einstellung auszunehmen.

  Bilder automatisch laden ist standardmäßig aktiviert.

- Deaktivieren Sie das Kontrollkästchen, um Bilder nicht automatisch zu laden. Dadurch werden die Browserseiten schneller aufgebaut. Auch hier können Sie **Ausnahmen** definieren.

Das **Downloadverzeichnis** kann hier definiert werden. Wenn Sie **Benutzerdefinierter Pfad** wählen, muss der genaue Pfad angegeben werden.

Aus Platzgründen sollten Sie keinen lokalen Pfad verwenden.

JavaScript aktivieren ist standardmäßig aktiviert. Die genauen Einstellungen können Sie hier definieren.

- Deaktivieren Sie das Kontrollkästchen, um JavaScript zu deaktivieren.
- Geben Sie unter **Sprachen für Webseiten** eine Liste mit Sprachen an in der Reihenfolge, wie Sie sie bei mehrsprachigen Webseiten anzeigen möchten. Verwenden Sie die offiziellen Sprachkürzel und trennen Sie sie mit Kommata. Wenn Sie das Feld leer lassen. wird die Standardsprache verwendet.

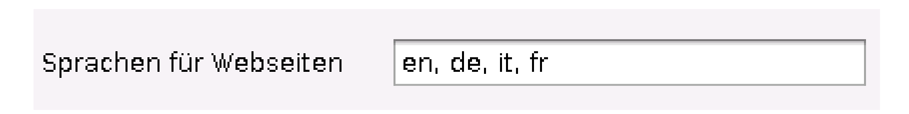


Figure 25: Sprachen für Webseiten angeben

Drucken

In diesem Bereich stellen Sie die **Standardpapiergröße** für den Drucker ein.



Figure 26: Einstellung der Papiergröße

Proxy

In diesem Bereich wählen Sie die Proxykonfiguration aus. Dabei haben Sie vier Möglichkeiten:

Direkte Verbindung zum Internet	Aktivieren Sie diese Option, um keinen Proxy zu verwenden.
Manuelle Proxykonfiguration	Konfigurieren Sie den Proxy individuell. Unter **Kein Proxy für** geben Sie eine Liste an, wofür Sie keinen Proxy benutzen möchten, z. B. `.mozilla.org, .net.de, .net.nz.` Unter Proxy-Realm geben Sie den Bereich an, für den der Proxy zuständig ist. Die Eingabe ist zwingend erforderlich, damit die automatische Anmeldung funktioniert. Lassen Sie die Felder **Proxy-Realm**, **Benutzername** und **Passwort** leer, um bei de Anmeldung die manuelle Eingabe zu ermöglichen.
Automatische Proxykonfiguration	Geben Sie die **URL** für die automatische Proxykonfiguration an.
Systemweite Proxykonfiguration	Verwenden Sie die Netzwerk/Proxy-Einstellungen aus dem IGEL Setup.

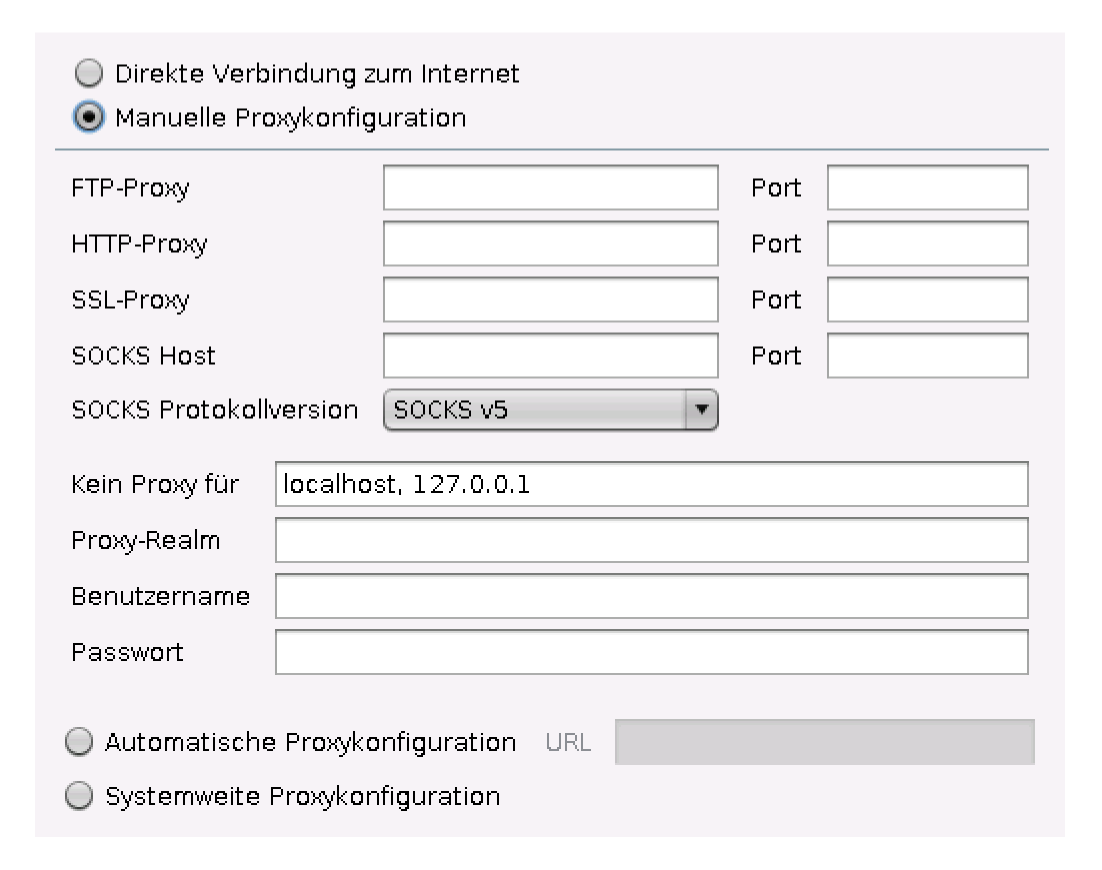


Figure 27: Proxyeinstellungen

Datenschutz

Zum Thema Datenschutz können Sie hier für folgende Bereiche Einstellungen vornehmen:

- *Private Daten* (Seite 49)
- *Schutz vor Verfolgung* (Seite 50)
- *Browser Adressleiste* (Seite 50)

Private Daten

In diesem Bereich legen Sie Einstellungen zur Browserchronik und zu privaten Daten fest.

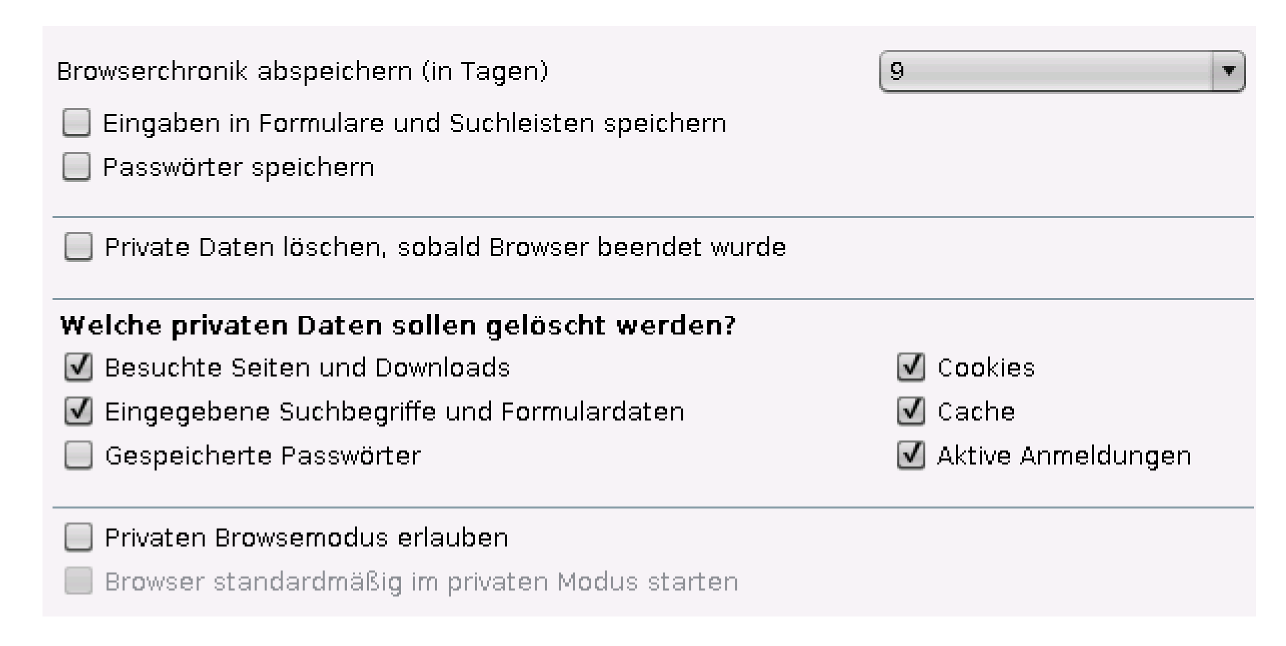


Figure 28: Datenschutzeinstellungen

- Definieren Sie ob, und wenn ja in wie viel Tagen sie die **Browserchronik** abspeichern wollen.

Die Chronik, die vor dem definierten Datum entsteht, geht bei Browserneustart verloren.

- Definieren Sie, ob Sie auch **Eingaben in Formulare und Suchleisten** oder **Passwörter** in der Chronik abspeichern wollen.
- Aktivieren Sie **Private Daten löschen sobald Browser beendet wurde**, wenn Sie die beim Surfen angefallenen Daten am Ende der Browsersitzung löschen wollen.
- Legen Sie genau fest, welche privaten Daten sie löschen wollen.
- Aktivieren Sie **Privaten Browsermodus erlauben**, um im Firefox den Privatmodus freizuschalten, bei dem keinerlei Daten gespeichert werden.
- Aktivieren Sie **Browser standardmäßig im privaten Modus starten**, um Firefox immer im Privatmodus zu öffnen.

Schutz vor Verfolgung

In diesem Bereich legen Sie fest, wie Sie sich vor Verfolgung im Internet schützen wollen.

☑ Nicht-Verfolgen-Funktion einschalten
☑ Tracking-Schutz aktivieren

Figure 29: Schutz vor Verfolgung

- Deaktivieren Sie die **Nicht-Verfolgen-Funktion**, wenn Sie Websites erlauben wollen, Ihre Aktivitäten zu verfolgen.

> Die **Do Not Track (DNT)-Funktion**, oder auch Nicht-Verfolgen-Funktion, ist standardmäßig eingeschaltet. Mit dieser Funktion teilen Sie einer Website mit, dass Sie nicht zu Zwecken wie verhaltensbasierter Werbung von Dritten verfolgt werden möchten. Dies geschieht, indem jedes Mal ein HTTP-Header von Do Not Track übertragen wird, wenn Sie Daten aus dem Internet anfordern. Hier entscheidet die besuchte Site, was sie mit dem Wunsch auf Privatsphäre macht.

- Deaktivieren Sie den **Trackingschutz**, wenn Sie den von Firefox bereitgestellten Schutz vor Verfolgung nicht nutzen möchten.

> Mit dem Schutz vor Verfolgung von Aktivitäten können Sie Ihre Online-Privatsphäre kontrollieren. Auch wenn Firefox eine **Nicht-Verfolgen-Funktion** beinhaltet, die Websites mitteilt, dass Sie das Aufzeichnen Ihres Surfverhaltens nicht wünschen, müssen sich Firmen nicht daran halten. Der Schutz vor Verfolgung von Aktivitäten in Firefox überlässt Ihnen die Kontrolle, indem solche Domains und Websites blockiert werden, die für das Verfolgen von Nutzern bekannt sind. Hier blockiert Firefox aktiv Inhalte, die das Surfverhalten des Nutzers mitzeichnen.

Adressleiste

Legen Sie hier weitere Regeln fest, um das Verhalten der Adressleiste auf ihre Bedürfnisse abzustimmen:

☑ Einträge aus der Chronik in der Adressleiste vorschlagen
  ☐ Nur direkt besuchte Einträge aus der Chronik vorschlagen
☑ Einträge aus den Lesezeichen in der Adressleiste vorschlagen
☑ Offene Tabs in der Adressleiste vorschlagen

Figure 30: Weitere Datenschutzeinstellungen

- Wollen Sie beim Eintippen einer URL Vorschläge aus **Chronikeinträgen** erhalten? Oder nur von Einträge, die Sie direkt eingetippt haben?
- Oder sollen Ihnen die Einträge aus den **Lesezeichen** vorgeschlagen werden?
- Sollen Ihnen bereits **geöffnete Tabs** als Ziel vorgeschlagen werden?

Sicherheit

In diesem Bereich legen Sie Einstellungen zu den Themen Phishing und Malware fest.

Alle Webseiten auf Echtheit prüfen ist standardmäßig nicht aktiviert.

➢ Aktivieren Sie dieses Kontrollkästchen, um den integrierten Phishingschutz einzuschalten.

Schutz gegen Malware ist standardmäßig nicht aktiviert.

➢ Aktivieren Sie dieses Kontrollkästchen, um Malware Blacklisten herunterzuladen und Downloads auf Malware zu überprüfen.

Erweitert

In diesem Bereich legen Sie Einstellungen zu Eingabeoptionen, Bildlauf und Webseiten fest.

☐ Alte Suchleiste verwenden
☐ Markieren von Text mit der Tastatur zulassen
☐ Suche bereits beim Eintippen starten
☐ Warnen wenn Webseiten versuchen weiterzuleiten oder neuzuladen
Rechtschreibung während der Eingabe prüfen: An für Textfelder

☐ Automatischen Bildlauf aktivieren
☐ Sanften Bildlauf aktivieren

☐ GStreamer-Unterstützung für den Browser deaktivieren
☐ OpenGL-Beschleunigung deaktivieren

Figure 31: Erweiterte Einstellungen

➢ Aktivieren Sie **Markieren von Text mit der Tastatur zulassen**, wenn Sie diese Funktion wünschen.

➢ Aktiveren Sie **Suche bereits beim Eintippen starten**, wenn Sie beim Tippen Suchvorschläge anzeigen lassen möchten.

➢ Wählen Sie **Rechtschreibung während der Eingabe prüfen** und bestimmen Sie, ob Sie dies nur für Testfelder oder auch Textzeilen wünschen.

➢ Wählen Sie **Automatischen Bildlauf aktivieren**, so können Sie die Ansicht einer Webseite durch Drücken der mittleren Maustaste und Bewegen der Maus in vertikaler Richtung im Anzeigebereich verschieben.

➢ Wählen Sie **Sanften Bildlauf aktivieren**, um zeilenweise oder pixelweise zu scrollen.

➢ Aktivieren Sie **Warnen wenn Webseiten versuchen weiterzuleiten oder neuzuladen**, wenn Sie dies wünschen.

➢ Aktivieren Sie **GStreamer-Unterstützung für den Browser deaktivieren**, falls Sie Wiedergabeprobleme von Videos bei HTML5-Webseiten haben.

➢ Aktivieren Sie **OpenGL_Beschleunigung deaktivieren**, falls Ihr Client Probleme mit OpenGL-Anwendungen hat.

Verschlüsselung

In diesem Bereich bestimmen Sie die Einstellungen für Verschlüsselungsprotokolle, Zertifikatsvalidierung und Autehntifizierungslösungen.

Verschlüsselungsprotokoll

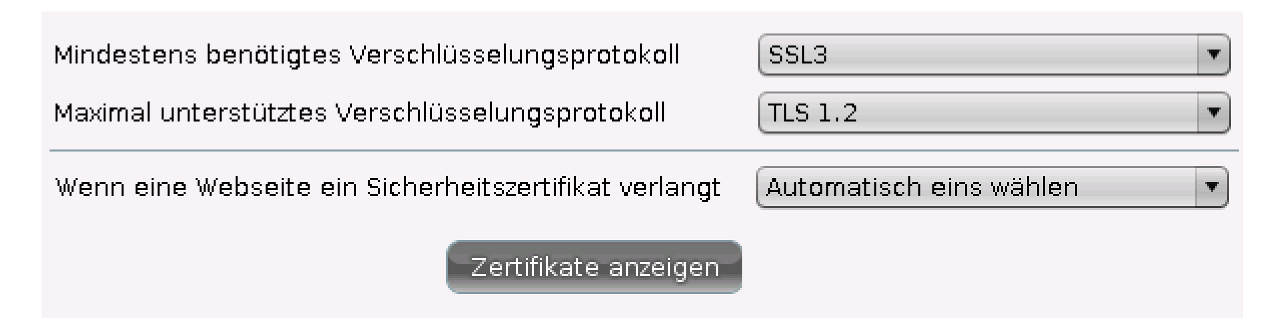


Figure 32: Verschlüsselungseinstellungen

- Wählen Sie ein minimales und maximales **Verschlüsselungsprotokoll**. Zur Auswahl stehen
  - **SSL3**
  - **TLS 1.0**
  - **TLS 1.1**
  - **TLS 1.2**
- Bestimmen Sie was zu tun ist, **wenn eine Webseite ein Sicherheitszertifikat verlangt**.
- Klicken Sie **Zertifikate anzeigen**, um die aktuell von Firefox verwendeten Zertifikate zu verwalten.

Zertifikatsvalidierung

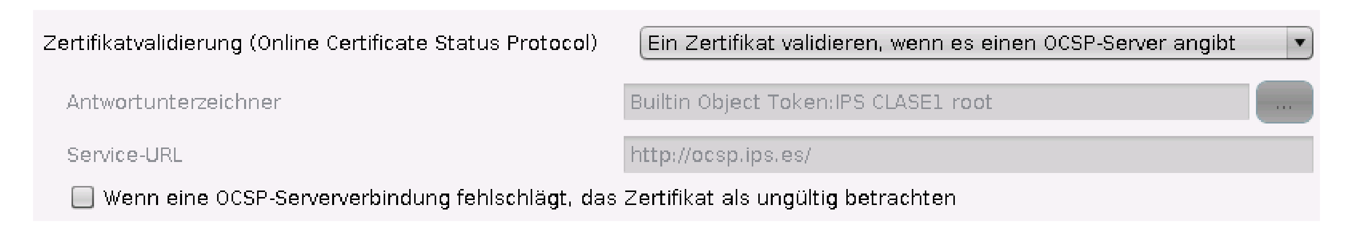


Figure 33: Zertifikatseinstellungen

- Definieren Sie die **Zertifikatsvalidierung**. Zur Auswahl stehen:
  - **Ein Zertifikat validieren, wenn es einen OCSP-Server angibt**
  - **Keine Zertifikatsvalidierung mit OCSP**
  - **Alle Zertifikate mittels des folgenden OCSP-Servers validieren**

    In diesem Fall müssen Sie den **Antwortunterzeichner** und die **Service-URL** angeben.

  Haben Sie eine Validierung mit OCSP ausgewählt, können Sie die Option **Wenn eine OCSP-Serververbindung fehlschlägt, das Zertifikat als gültig betrachten** aktivieren.

Authentifizierung

➢ Wählen Sie aus folgenden Produkten die Authentifizierungslösung zum Schutz Ihres Netzwerks:

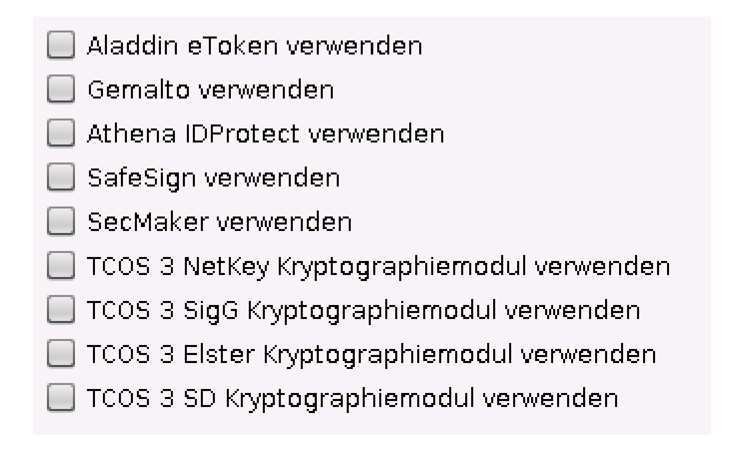


Figure 34: Authentifizierungslösungen

Kommandos

In diesem Bereich geben Sie Einstellungen für bestimmte Kommandos ein.

➢ Klicken Sie ein Kommando., um die Schaltfläche **Bearbeiten** zu aktivieren.



Figure 35: Einstellung für Kommandos

5.8.2. Firefox Browsersitzungen

Die Originalparameter von Firefox sind voreingestellt. Die Standardeinstellungen werden vom Setup **Browser Global** übernommen.

Darüber hinaus können die folgenden Einstellungen für die **Browsersitzung** konfiguriert werden:

- *Fenstereinstellungen* (Seite 54)
- *Menüs & Symboleisten* (Seite 54)
- Listenelemente
- Symbolleiste konfigurieren
- *Hotkeys* (Seite 57)
- *Kontextmenü* (Seite 57)
- Desktopintegration

Fenstereinstellungen

In diesem Bereich nehmen Sie die Fenstereinstellungen für eine Browsersitzung vor.

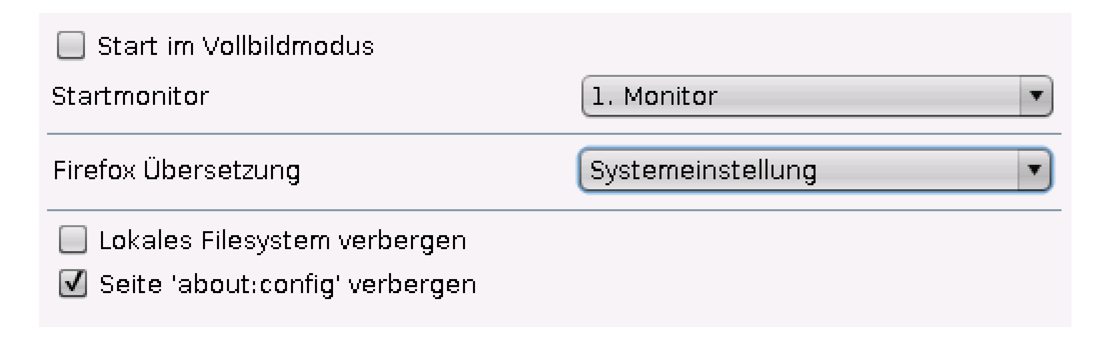


Figure 36: Fenstereinstellungen

Der **Vollbildmodus** ist standardmäßig ausgeschlatet.

➢ Aktivieren Sie das Kontrollkästchen, um den Vollbildmodus einzuschalten.

Wenn Sie mehrere Monitore angeschlossen haben können Sie hier den **Startmonitor** festlegen.

➢ Wählen Sie unter **Firefox Übersetzung** die Sprache, in die die Benutzeroberfläche von Firefox übersetzt werden soll.

➢ Aktivieren Sie **Lokales Filesystem verbergen**, wenn sie beim Abspeichern von Dateien nicht die lokale Struktur anzeigen lassen möchten.

Menüs & Symbolleisten

In diesem Bereich können Sie die Firefox Menüs und Symbolleisten an Ihre persönlichen Bedürfnisse anpassen, indem Sie

- Elemente der Menüleiste verbergen
- Listenelemente verbergen
- Symbolleiste konfigurieren

➢ Aktivieren Sie **Benutzerkonfiguration der Symbolleisten**, um dem Benutzer zu erlauben, Symbolleisten zu konfigurieren.

➢ Konfigurieren Sie die **Navigationssymbolleiste**.

Voreingestellt sind folgende Elemente:

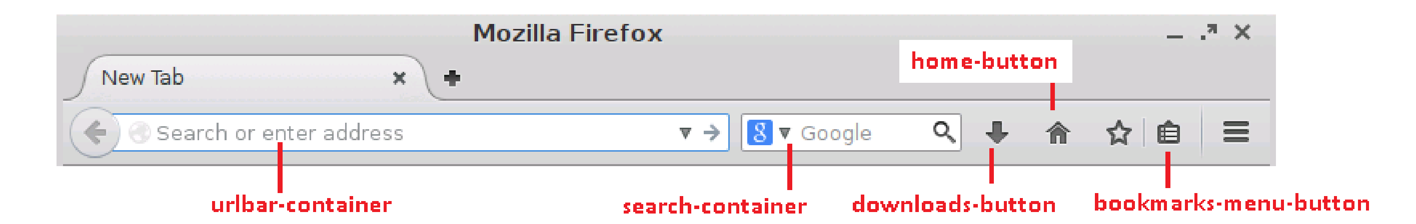


Figure 37: Navigationssymbolleiste

➢ Konfigurieren Sie das **Applikationsmenü:**

Voreingestellt sind diese Elemente:

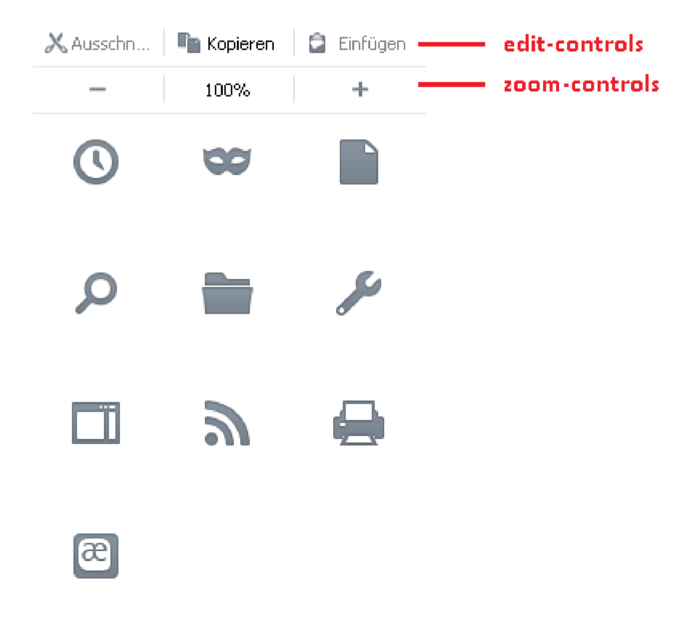
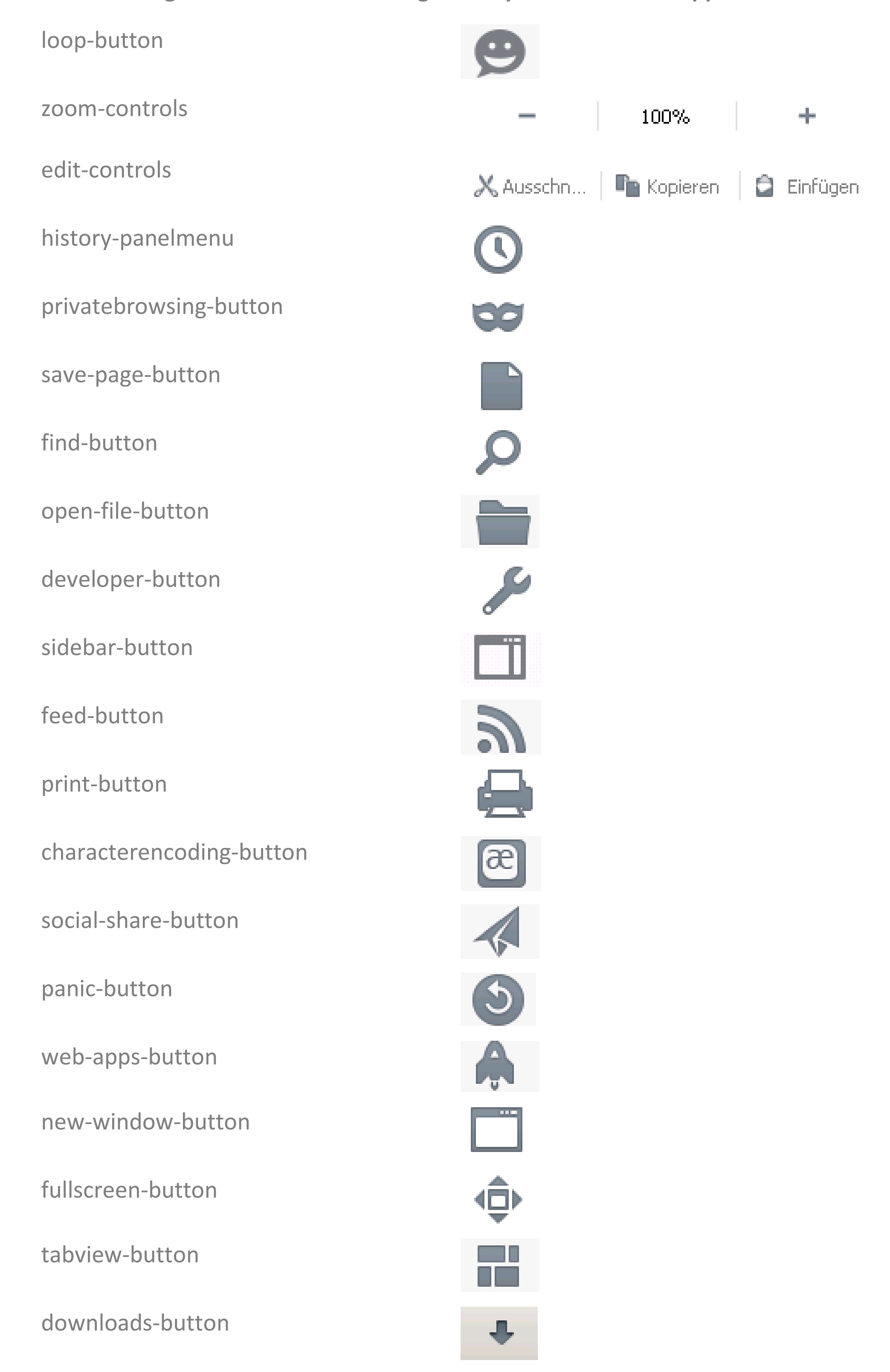


Figure 38: Applicationsmenü

Beachten Sie, dass einige Elemente nur angezeigt werden, wenn das das dazugehörige Feature aktiviert ist.

- Konfigurieren Sie das **Applikationsmenü:**
- **Weitere mögliche Elemente für Navigationssymbolleiste und Applikationsmenü sind:**



- Klicken Sie **Standardsymbolkonfiguration wiederherstellen**, um Ihre Änderungen rückgängig zu machen.

Hotkeys

In diesem Bereich können Sie folgende Firefox-Hokeys deaktivieren:

Folgende Elemente deaktivieren

- [ ] Hotkey für 'Beenden/Schließen' deaktivieren
- [ ] Hotkey für Druckdialog deaktivieren
- [ ] Hotkey für 'Seite abspeichern' deaktivieren
- [ ] Hotkeys zum Öffnen eines neuen Fensters/Tabs deaktivieren
- [ ] Hotkeys zum Öffnen einer neuen Website/Location und des Downloadfensters deaktivieren
- [ ] Hotkeys zum Anzeigen der Chronik und Seiteninformationen deaktivieren
- [ ] Hotkeys zum Anlegen eines Lesezeichens deaktivieren
- [ ] Hotkeys zum Abzeigen der Hilfe deaktivieren
- [ ] Hotkeys zum Starten des Caret Browsing deaktivieren

Figure 39: Einstellungen zu Hotkeys

Kontextmenü

In diesem Bereich können Sie verschiedene Elementen des Browser-Kontextmenüs deaktivieren.

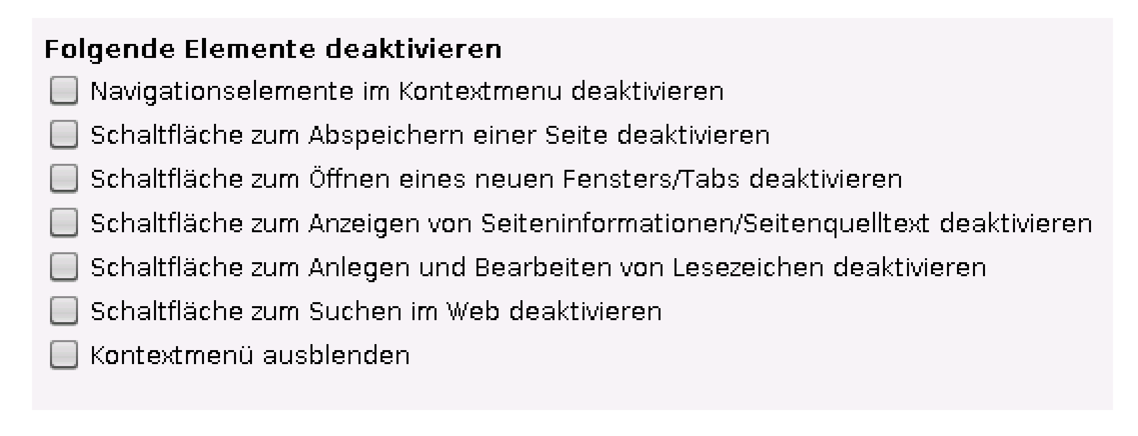


Figure 40: Einstellungen zum Kontextmenü

5.8.3. Browser-Plug-ins

Hier stehen folgende Plug-ins zur Verfügung:

- Adobe Flash Player
- PDF-Betrachter
- Red Hat Spice

Diese müssen ggf. vom Anwender erst lizenziert werden.

Das Browser-Plug-in des Media Players konfigurieren Sie unter **Media Player Global→Browser Plug-in** **(Seite 61).**

Flash

Bevor Sie Adobe Flash Player herunterladen und installieren können, müssen Sie die Lizenzierung der Software bestätigen - IGEL Linux enthält keine Lizenz für die Verwendung des Flash Players.

➢ Setzen Sie ein Häkchen im Kontrollkästchen **Ich will den Flash Player selbst lizenzieren**, um die Seite **Download Flashplayer** zu aktivieren.

Der externe Link zum Download des Flashplayers ist aktuell zum Zeitpunkt der Veröffentlichung dieser Software, er kann sich jedoch im Laufe der Zeit ändern.

Neben der offiziellen Downloadquelle können Sie auch eine eigene Quelle im Firmennetzwerk angeben oder die bereits konfigurierte Quelle der Firmware Updates verwenden.

> Wenn das Herunterladen des Flash Players über den externen Link fehlschlägt, überprüfen Sie selber im Browser den aktuellen Pfad und Dateinamen, da sich dieser zwischenzeitlich geändert haben kann.

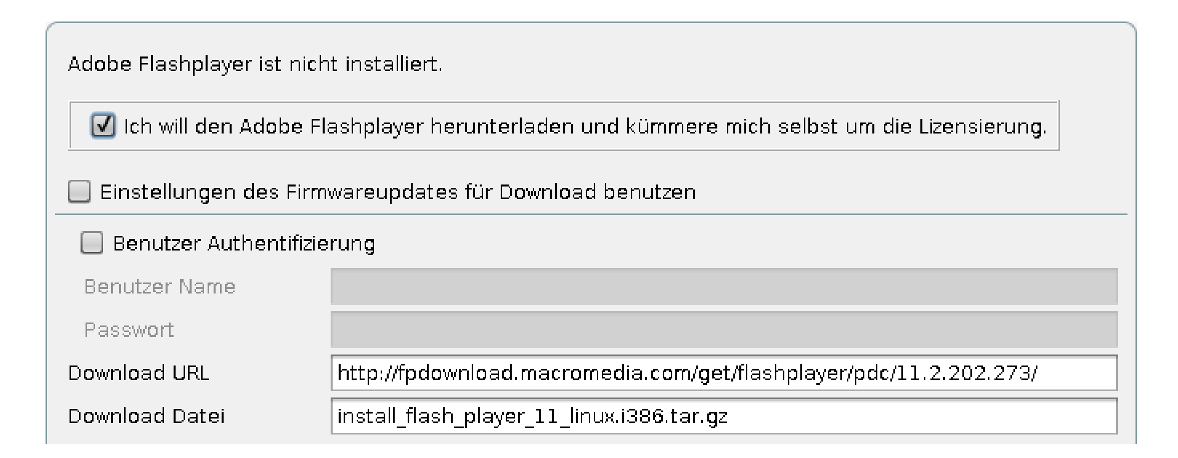


Figure 41: Adobe Flash Player

PDF-Betrachter

Stellen Sie hier ein, ob PDF-Dokumente in den Browser eingebettet werden sollen, oder ob sie in einem separaten Fenster dargestellt werden sollen.

RedHat Spice

In diesem Bereich nehmen Sie Einstellungen zu virtuellen Umgebungen vor.

➢ Aktivieren Sie **Browserplugin erlauben**, um virtuelle Desktopumgebungen überall über das Internet anzuzeigen.

➢ Aktivieren oder deaktivieren Sie **USB-Geräte weiterleiten**.

5.9. Media Player

Richten Sie hier für Ihre Multimedia Anwendungen den Media Player nach ihren Wünschen ein.

Folgende Codecs sind entweder über das Fluendo Codec Pack oder durch das MPEG LA Advanced Feature Pack lizenziert:

Unterstützte Formate:	Unterstützte Codecs:
AVI MPEG ASF (eingeschränkt unter Linux) WMA WMV (eingeschränkt unter Linux) MP3 OGG	MP3 WMA stereo WMV 7/8/9 MPEG 1/2 MPEG4 H.264

AC3 ist nicht lizenziert.

Ab IGEL Linux 5.06.100 ist auf bestimmten Geräten Hardwarebeschleunigung für Multimedia-Wiedergabe verfügbar. Näheres entnehmen Sie einem FAQ-Dokument zum Thema.

5.9.1. Media Player Global

➢ Nehmen Sie allgemeingültige Einstellungen vor, die standardmäßig für alle Media Player Sitzungen gültig sein sollen.

In den einzelnen Sitzungen können diese Einstellungen bei Bedarf geändert werden.

Fenster

➢ Geben Sie unter **Bildseitenverhältnis** das gewünschte Seitenverhältnis der Videodarstellung an.

Zusätzlich können Sie folgende Optionen wählen:

- Vollbildmodus
- Fenstergröße automatisch ändern, sobald ein neues Video geladen wird
- Hauptfenster soll im Vordergrund bleiben
- Bedienelemente anzeigen

Playback

➢ Bestimmen Sie, auf welche Weise Sie Mediadateien abspielen möchten:

Endlosschleife	Spielt eine Playlist automatisch immer wieder ab, bis Sie sie stoppen.
Zufallsmodus	Spielt die Dateien einer Playlist per Zufallsgenerator ab.

➢ Wählen Sie bei Bedarf visuelle Effekte, die während der Audiowiedergabe abgespielt werden.

Visualisierungstyp	Bestimmt den Visualisierungs-Plug-in.
Visualisierungsgröße	Bestimmt die Visualisierungsgröße.

Video

Videoausgabe	**GConf:**	systemweite Konfiguration
	Auto:	automatische Auswahl der Ausgabe
	XVideo:	hardwarebeschleunigt, indem mittels shared memory Bilder in den Speicher der Grafikkarte geschrieben werden.
	X11:	nicht hardwarebeschleunigt, Darstellung über das Anzeigeprotokoll X Window System.

➢ Bestimmen Sie die Videoeinstellungen Helligkeit, Sättigung, Kontrast und Farbton.

Audio

Audioausgabe	**GConf:**	systemweite Konfiguration
	Auto:	automatische Auswahl der Ausgabe
	ALSA:	direkte Ausgabe über Kerneltreiber für Soundkarten
Audioausgabetyp	Wählen Sie hier Stereo aus, wenn Sie mit einem IGEL Thin Client arbeiten.	

Optionen

➢ Bestimmen Sie, ob Sie den **Bildschirmschoner** bei Audiowiedergabe deaktivieren wollen.

➢ Legen Sie die **Geschwindigkeit der Netzwerkverbindung** fest, um Einfluss auf die Wiedergabe der Media-Dateien zu nehmen.

➢ Bestimmen Sie eine **Puffergröße**, die in Ihrem Netzwerk nötig ist, um fließende Ton- und Bildwiedergabe zu ermöglichen.

➢ Legen Sie fest, ob Sie **Untertitel automatisch laden** wollen, sobald ein Video gestartet wird. Die **Kodierung** der Untertiel ist derzeit immer UTF-8.

➢ Bestimmen Sie die **Schriftart** und **Schriftgröße** der Untertitel.

Browser-Plug-in

Wenn Sie den Media Player als **Browser-Plug-in** verwenden möchten, können Sie hier die Konfigurationswerte ändern.

Dies hat Auswirkungen auf manuell konfigurierte Media Player-Sitzungen.

5.9.2. Media Player Sitzungen

Hier richten Sie Ihre ganz persönlichen Media-Player-Sitzungen ein.

1. Klicken Sie **Hinzufügen**, um eine neue Sitzung anzulegen.
2. Vergeben Sie einen **Sitzungsnamen.**
3. Geben Sie an, welche **Startmöglichkeiten der Sitzung** sie wünschen. Hier ist eine Mehrfachauswahl möglich.
4. Wählen Sie eventuell die Möglichkeit, **Hotkeys** zu verwenden und definieren Sie diese.
5. Außerdem können Sie angeben, ob Sie **Autostart** nach Systemstart und/oder **Neustart** nach Verbindungsaufbau wünschen.
6. Für die Autostartoption können Sie zusätzlich angeben, um wie viele Sekunden der Sitzungsstart verzögert werden soll.

Sobald Sie eine eigene Media-Player-Sitzung eingerichtet haben, erscheint diese im Strukturbaum unter dem Verzeichnis **Media Player Sitzungen**. Ihre eigenen Sitzung enthält wiederum die drei Ordner **Playback**, **Optionen** und **Arbeitsflächenintegration**.

Playback

➢ Geben Sie unter **Medium / Datei** den Pfad der Datei an, die abgespielt werden soll, wenn diese Sitzung gestartet wird. Verwenden Sie dazu folgende Formate:

  `/directory/filename`
  oder
  `http://servername/filename`.

Für die Fenstereinstellungen können Sie hier wählen, ob sie die Vorgaben der globalen Einstellungen übernehmen möchten, oder für diese spezielle Sitzung eigene Modi verwenden möchten.

Optionen

Hier können Sie gegebenenfalls die Voreinstellung zu den Bedienelementen ändern.

5.10. Java Web Start Sitzung

Um auf Java Web Start-Anwendungen zugreifen zu können, müssen Sie die Adresse der erforderlichen JNLP-Datei eingeben. Dies kann z.B. eine IGEL UMS Konsole sein, die sich ebenfalls als Java Web Start-Anwendung ausführen lässt.

5.11. VNC-Viewer

Legen Sie eine **VNC-Viewer-Sitzung** an, um über den Thin Client auf entfernte Rechner (VNC-Server) zugreifen zu können. Verbindungsoptionen wie die Serveradresse oder der Vollbildmodus lassen sich für jede Sitzung vorbelegen oder auch beim Sitzungsstart individuell definieren.

> Wird für die Sitzung eine Serveradresse festgelegt, so erscheint der Verbindungsdialog beim Start der Sitzung nicht, die Verbindung wird direkt aufgebaut.

6. Zubehör

Hier finden Sie Informationen zu weiterem Zubehör, das IGEL Linux zur Verfügung stellt. Die meisten dieser Funktionen können wie Sitzungen bereitgestellt werden (Desktop, Startmenü usw.).



Figure 42: Zubehör

6.1. ICA Connection Center

Das Citrix ICA Connection Center bietet eine Übersicht der bestehenden Verbindungen zu Citrix Servern und erlaubt unter anderem das Trennen und Abmelden der Serververbindung und die Anzeige der Verbindungseigenschaften, z.B. zu Supportzwecken.

6.2. Terminals

Mit einer Terminal Sitzung können Sie lokale Befehle über eine Shell ausführen.

> Auf eine lokale Shell kann auch ohne Terminal Sitzung zugegriffen werden: Wechseln Sie mit Strg+Alt+F11 bzw. Strg+Alt+F12 zu den virtuellen Terminals tty11 bzw. tty12.

6.3. Smartcardpasswort ändern

Legen Sie eine Sitzung an zum Ändern des Passworts Ihrer IGEL Smartcard. Die Einrichtung der IGEL Smartcard finden Sie im Setup unter **Sicherheit→Anmeldung→Smartcard**.

6.4. Smartcard personalisieren

In der Personalisierung können Sie ein Anmeldepasswort festlegen und Sitzungen zur Karte hinzufügen.

Sitzungskonfigurationen werden auf dem IC (integrierter Schaltkreis) der Karte gespeichert, und die Sitzung kann auf jedem beliebigen IGEL Thin Client verwendet werden, der die Karte liest.

6.5. Setupsitzung

Dem Benutzer können bestimmte Bereiche des Setups zur Verfügung gestellt werden, auch wenn das Setup insgesamt nur dem Administrator zugänglich ist. Dies ist z. B. sinnvoll für Tastatur- und Mauseinstellungen oder die Bildschirmkonfiguration.Siehe *Setupseiten für Benutzer freigeben* (Seite 19).

6.6. Quicksetupsitzung

Dem Benutzer können bestimmte Bereiche des Setups zur Verfügung gestellt werden, auch wenn das Setup insgesamt nur dem Administrator zugänglich ist. Dies ist z. B. sinnvoll für Tastatur- und Mauseinstellungen oder die Bildschirmkonfiguration.Siehe *Quicksetup* (Seite 19).

6.7. Bildschirm umschalten

In diesem Bereich können Sie Einstellungen für das Umschalten von Bildschirmgeräten vornehmen.

Standardmäßig ist die Bildschirmauswahl nicht aktiviert.

- ➢ Aktivieren Sie die Bildschirmauswahl, indem Sie unter **Zubehör→Bildschirm umschalten** eine der **Startmöglichkeiten der Sitzung** aktivieren.
- ➢ Aktivieren Sie **Benutze Hotkeys**, um für diese Sitzung einen Hotkey oder ein Icon zu bestimmen.
- ➢ Geben Sie gegebenenfalls Autostartoptionen an.

➢ Gehen Sie auf **Zubehör→Bildschirm umschalten→Optionen**, um folgende Einstellungen vorzunehmen:

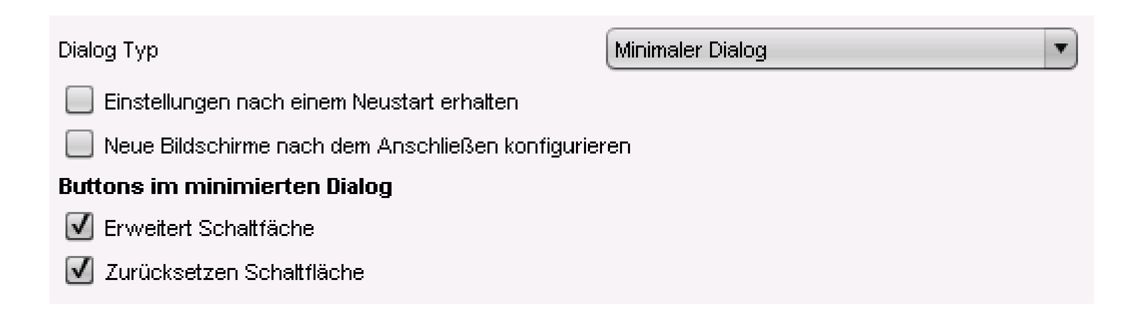


Figure 43: Einstellungen zum Umschalten der Bildschirme

➢ Geben Sie unter **Dialogtyp** an, wie der Bildschirmauswahldialog aussehen soll:

Minimaler Dialog	Funktioniert nur mit zwei Displays.
Erweiterter Dialog	Der Benutzer kann Auflösung oder Rotation außerhalb des Setups selber ändern.

➢ Aktivieren Sie **Neue Bildschirme nach dem Anschließen konfigurieren**, um Einstellungen vornehmen zu können für neu angeschlossene Geräte, die während des Betriebs angeschlossen werden.

➢ Aktivieren Sie **Einstellungen nach einem Neustart erhalten**, um die Bildschirmeinstellungen abzuspeichern, dass sie bei einem Neustart weiterverwendet werden können.

➢ Legen Sie die Schaltflächen für den minimalen Dialog fest:

Erweitert	Ermöglicht im minimalen Dialog den Sprung zum erweiterten Dialog.
Zurücksetzen	Setzt die Konfiguration auf Setupeinstellungen zurück.

6.8. Starter für Sitzungen

➢ Lassen Sie **Setup** und **Starter für Sitzungen** auf dem lokalen Desktop oder im Startmenü eingeblendet oder definieren Sie Hotkeys und die Autostartoption.

Sie können einige Elemente wie Schaltflächen für das Herunterfahren oder den Neustart des Geräts vor dem Benutzer verbergen.

6.9. Audioeinstellungen

Konfigurieren Sie unter **Zubehör→Audioeinstellungen→Optionen** die Lautstärke für Tonausgabe und Tonaufnahme.

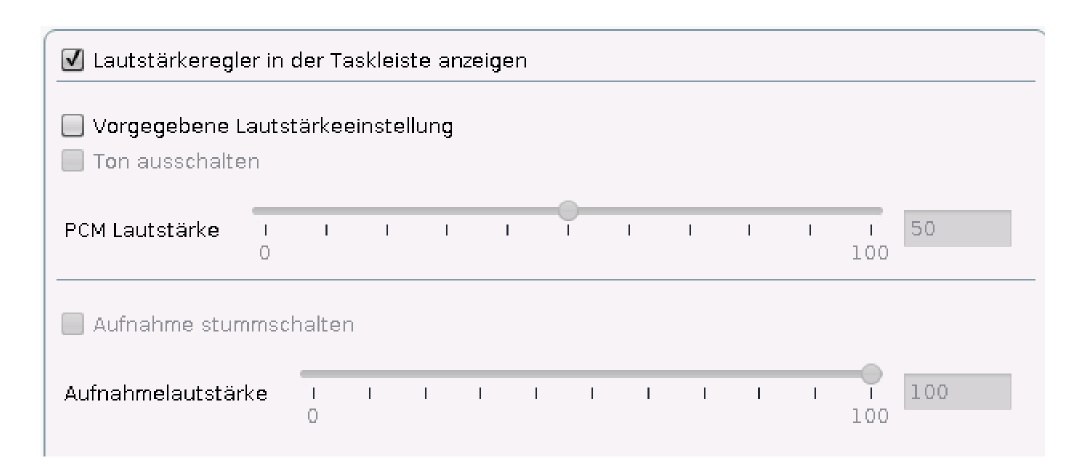


Figure 44: Soundsteuerung

- Aktivieren Sie **Lautstärkeregler in der Taskleiste anzeigen**, um die Tonausgabeeinstellungen in der Taskleiste anzuzeigen.
- Klicken Sie **Vorgegebene Lautstärkeregelung** um die PCM Lautstärke und die Aufnahmelautstärke einzustellen.

  Diese Einstellungen werden bei jedem Systemstart übernommen.
- Aktivieren Sie die Stummschaltung für Tonausgabe oder Aufnahme.

Seien Sie sehr vorsichtig bei der Voreinstellung der Aufnahmelautstärke, hier kann man viel falsch machen. Normalerweise stellt der Benutzer die Lautstärke je nach individueller Umgebung selber ein.

6.10. Systemprotokolle

Alle verfügbaren Systemprotokolle werden aktualisiert angezeigt. Eigene Logdateien können in den Optionen hinzugefügt werden. Der Inhalt eines ausgewählten Protokolls lässt sich im Betrachter durchsuchen und auch (z.B. für Supportzwecke) kopieren.

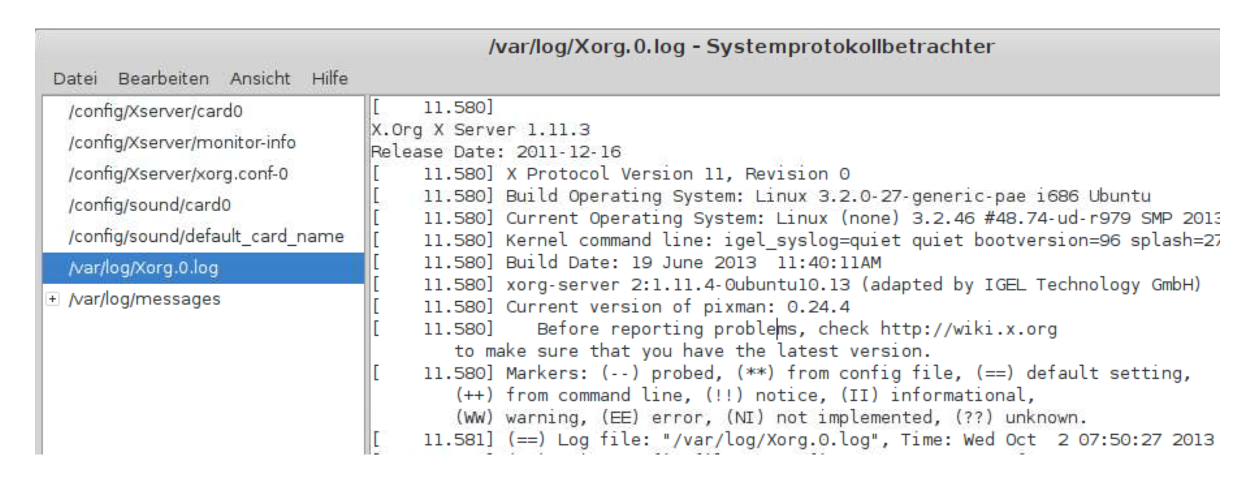


Figure 45: Systemprotokolle

6.11. UMS-Registrierung

Die Registrierung des Thin Clients in der IGEL Universal Management Suite kann auch auch lokal ausgeführt werden. Geben Sie dazu die Serveradresse mit Port und die notwendigen Zugangsdaten an. Am Server bestehende Verzeichnisse können direkt angewählt werden.



Figure 46: Thin Client am UMS Server registrieren

6.12. Touchscreenkalibrierung

Nachdem das Kalibrierungsprogramm gestartet wurde, wird ein Muster mit Kalibrierungspunkten angezeigt, die nacheinander berührt werden müssen.

6.13. Bildschirmtastatur

Aktivieren Sie die Bildschirmtastatur für die Verwendung mit der Maus oder einem Touchscreen, z. B. IGEL UD10.



Figure 47: Bildschirmtastatur

6.14. Java Control Panel

Das Java Control Panel ist eine Bedienkonsole, die für unterschiedliche Zwecke eingesetzt wird.

- Definieren Sie über verschiedene Parameter, wie Java auf Ihrem Computer ausgeführt wird.
- Verwalten Sie für Java Plug-in verwendete temporäre Dateien.

  Dadurch kann Ihr Webbrowser Sun Java verwenden, um Applets und Java Web Start auszuführen, wodurch Sie Java-Anwendungen über das Netzwerk starten können.
- Kontrollieren Sie Zertifikate über die Bedienkonsole. So erhalten Sie Sicherheit für die Nutzung von Applets und Anwendungen über das Netzwerk.
- Definieren Sie Laufzeitparameter für mit Java-Plug-in ausgeführte Applets und für mit Java Web Start ausgeführte Anwendungen.

Weitere Informationen hierzu finden Sie unter http://java.sun.com/j2se/1.5.0/docs/guide/deployment/deployment-guide/jcp.html.

6.15. Kalibrierungsmuster

Für die Monitorkalibrierung (Auto Adjust) verwenden Sie bitte dieses spezielle Muster – dies führt in der Regel zu besseren Ergebnissen als eine Kalibrierung mit einer üblichen Arbeitsfläche und Fenstern. Ein Mausklick auf das Muster schließt die Anwendung wieder.

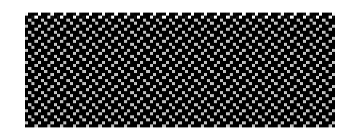


Figure 48: Kalibrierungsmuster

6.16. Befehle

Dem Benutzer können folgende Systembefehle zugänglich gemacht werden:

- **Abmelden**
- **Symbole sortieren**
- **Terminal ausschalten**
- **Terminal neu starten**
- **Windowmanager neu starten**

6.17. Netzwerkdiagnose

Die IGEL Linux Firmware umfasst einige Tools für die Netzwerkanalyse, darunter:

- *Geräteinformationen*
- *Ping*
- *Netstat*
- *Traceroute*
- *Look-up*

6.17.1. Geräteinformationen

Dieses Tool liefert Informationen zum Status des verwendeten Netzwerkgeräts, u. a.:

- MAC- und IP-Adresse
- Link Speed (Verbindungsgeschwindigkeit)
- einige Schnittstellenstatistiken (übertragene Byte, Fehler etc.)

6.17.2. Ping

Mit dem **Ping**-Tool senden Sie Kontaktanfragen an eine Netzwerkadresse. Sie können die Anzahl der zu sendenden Anfragen genau festlegen oder sie aktivieren **Unlimited requests**, dann werden die Echoaufforderungen solange gesendet, bis Sie den Prozess anhalten.

Das Ping-Ergebnis wird unten angezeigt, und die Ping-Dauer der letzten fünf Pings wird in einem Balkendiagramm dargestellt.

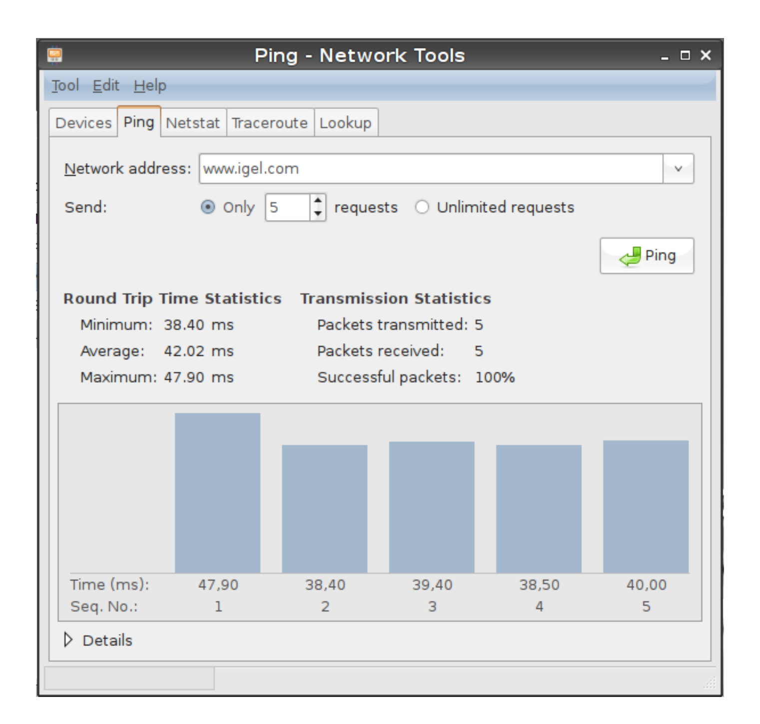


Figure 49: Ping-Network-Tools

- Aktivieren Sie in der Menüleiste **Programm→Signalton beim Ping**, um den Thin Client so zu konfigurieren, dass er bei jedem versendeten Ping ein akustisches Signal ausgibt.

6.17.3. Netstat

Netstat liefert Informationen zu aktiven Netzwerkservices mit Protokoll- und Portinformationen sowie einer Routingtabelle und Multicast-Informationen zu Ihren Netzwerkgeräten.

6.17.4. Traceroute

Mit **Traceroute** können Sie die Strecke zu einer Netzwerkadresse nachverfolgen.

6.17.5. Look-up

Das **Look-up**-Tool zeigt unterschiedliche Informationen zu einer Netzwerkadresse an. Die verfügbaren Informationstypen sind auf diesem Screenshot dargestellt.

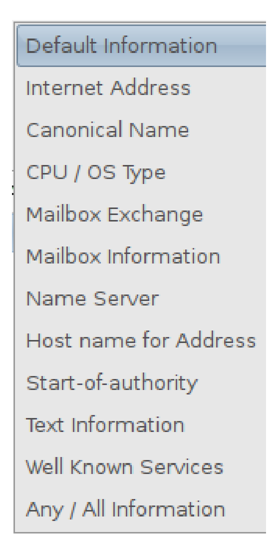


Figure 50: Informationstypen für Netzwerkadresse

6.18. Systeminformationen

Die Systeminformationen bieten eine Übersicht auf alle internen und angeschlossenen Hardwarekomponenten des Thin Clients sowie die Bestandteile des Linux Systems (z.B. Kernel Module). Die angezeigten Informationen lassen sich in die Zwischenablage kopieren, um sie z.B. dem IGEL Support zukommen zu lassen.

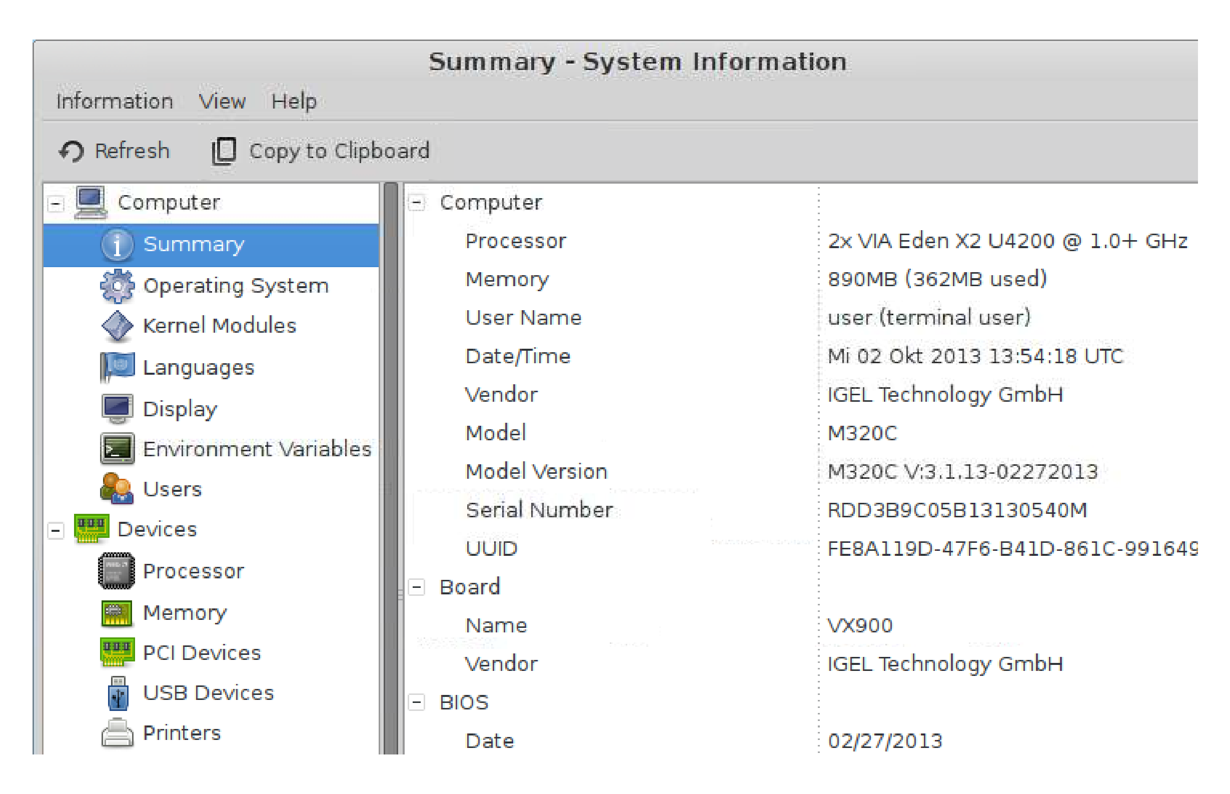


Figure 51: Systeminformationen

6.19. Laufwerksverwaltung

In der Laufwerksverwaltung werden alle erkannten USB-Laufwerke angezeigt mit ihren jeweiligen Eigenschaften (Gerätename, Mountpoint usw.).

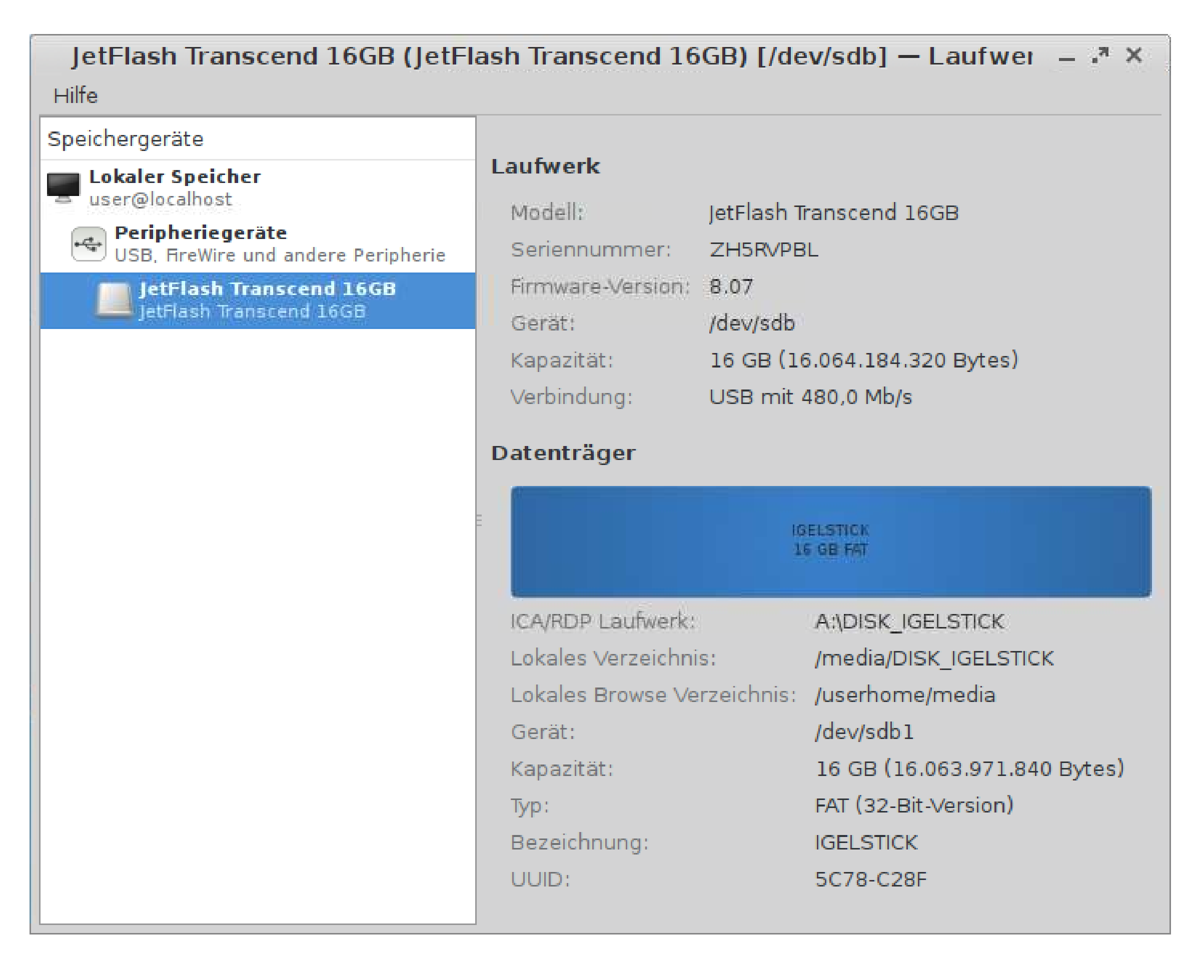


Figure 52: Laufwerksverwaltung

Ist *Dynamic Client Drive Mapping* (Seite 109) aktiviert, lassen sich angeschlossene Speichergeräte in der Laufwerksverwaltung sicher entfernen:

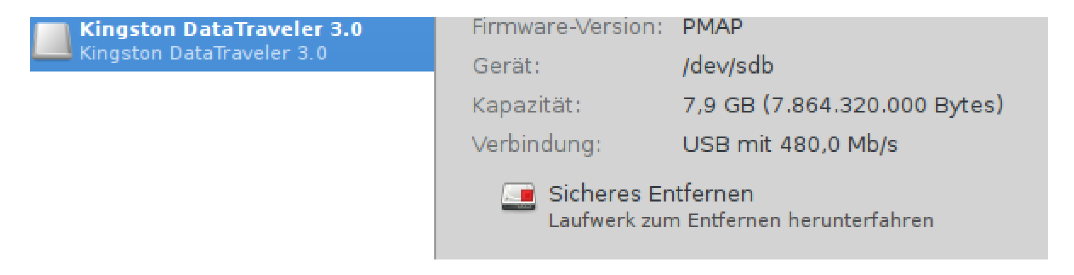


Figure 53: Sicheres Entfernen

Aktivieren Sie im Setup unter **Zubehör→Laufwerksverwaltung** die Option **Benutze Hotkey**, um die Laufwerksverwaltung mit einer Tastenkombination aufrufen zu können, beispielsweise in Vollbildsitzungen. Wählen Sie dazu einen **Modifier** und einen **Hotkey**.

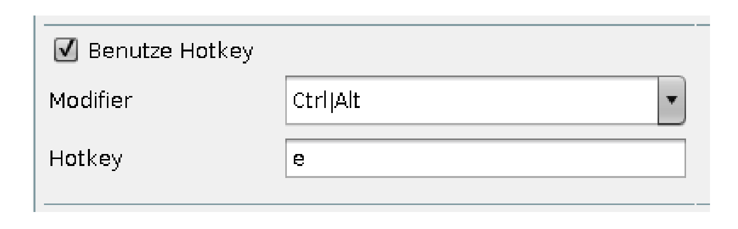


Figure 54: Benutze Hotkey

6.20. Firmwareupdate

Diese Sitzung Aktualisiert die Firmware mit den in **System→Update→Firmwareupdate** gespeicherten Einstellungen.

6.21. Bildschirme identifizieren

Zeigt auf jedem angeschlossenen Bildschirm die Bildschirmnummer des IGEL Setups und Informationen zur Hardware an.

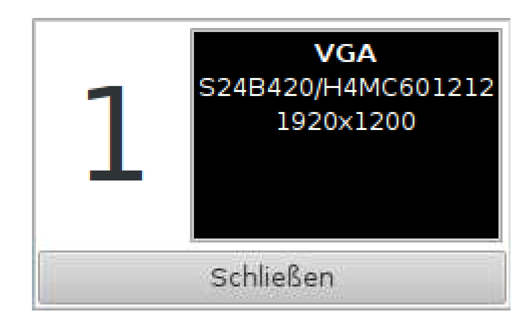


Figure 55: Bildschirme identifizieren

6.22. Lizenzupgrade

Sie können zusätzliche Funktionen der Firmware entweder über die IGEL Universal Management Suite verteilen oder die Lizenzen auch lokal am Thin Client einspielen. Dazu muss entweder ein IGEL USB-Stick mit Smartcard am System eingesteckt sein oder aber ein Speichermedium mit bereits erstellten Lizenzen für dieses Gerät.



Figure 56: Upgrade der Firmwarelizenz

6.23. Webcam Information

Das **Webcam Information** Werkzeug liest aus einer angeschlossenen Webcam Informationen aus wie Hersteller, Modell und unterstützte Videoformate. Außerdem lässt sich ein Testbild der Kamera mit gewählten Einstellungen anzeigen.

- Starten Sie **Webcam Information** im **Starter für Anwendungen** (**System**).
- Wählen Sie eine Auflösung und klicken Sie **Testen**, um das Kamerabild anzuzeigen.



Figure 57: Webcam Information

> Eine Liste mit allen unterstützten Videoformaten lässt sich in der Linux Konsole erzeugen mit dem Befehl: `webcam-info -l`.

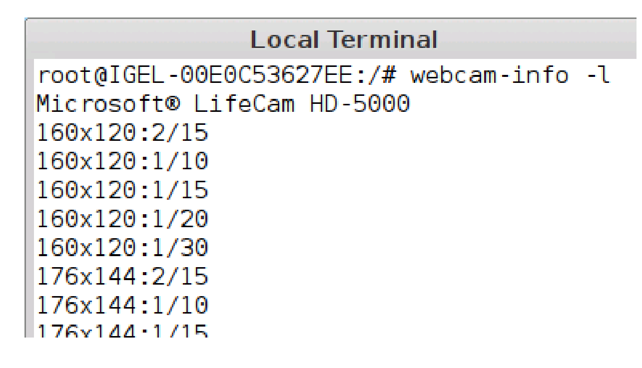

Local Terminal
```
root@IGEL-00E0C53627EE:/# webcam-info -l
Microsoft® LifeCam HD-5000
160x120:2/15
160x120:1/10
160x120:1/15
160x120:1/20
160x120:1/30
176x144:2/15
176x144:1/10
176x144:1/15
```

Figure 58: Befehl webcam-info -l

- ➢ Um die Funktion der Webcam in einer Sitzung zu prüfen (z.B. über Citrix HDX Webcam Redirection umgeleitet), rufen Sie im Browser innerhalb der Sitzung die Webseite *cameroid.com* (*Webcam Testseite cameroid.com*) auf (Adobe Flash muss installiert sein).

6.24. Bildbetrachter

Der Bildbetrachter GPicview dient ab IGEL Universal Desktop Linux 5.06.100 zum Betrachten einer Vielzahl von Grafik-MIME-Typen:

- image/bmp
- image/gif
- image/jpeg
- image/jpg
- image/png
- image/x-bmp
- image/x-pcx
- image/x-tga
- image/x-portable-pixmap
- image/x-portable-bitmap
- image/x-targa
- image/x-portable-greymap
- application/pcx
- image/svg+xml
- image/svg-xml

Wie Sie diese Zuordnung ändern können, erklärt ein *FAQ-Eintrag* (*https://faq.igel.com/otrs-igel/public.pl?Action=PublicFAQZoom;ItemID=680*).

Bedienungshinweise zum Bildbetrachter finden Sie auf *dieser Webseite der Ubuntu Users.* (*http://wiki.ubuntuusers.de/GPicview*)

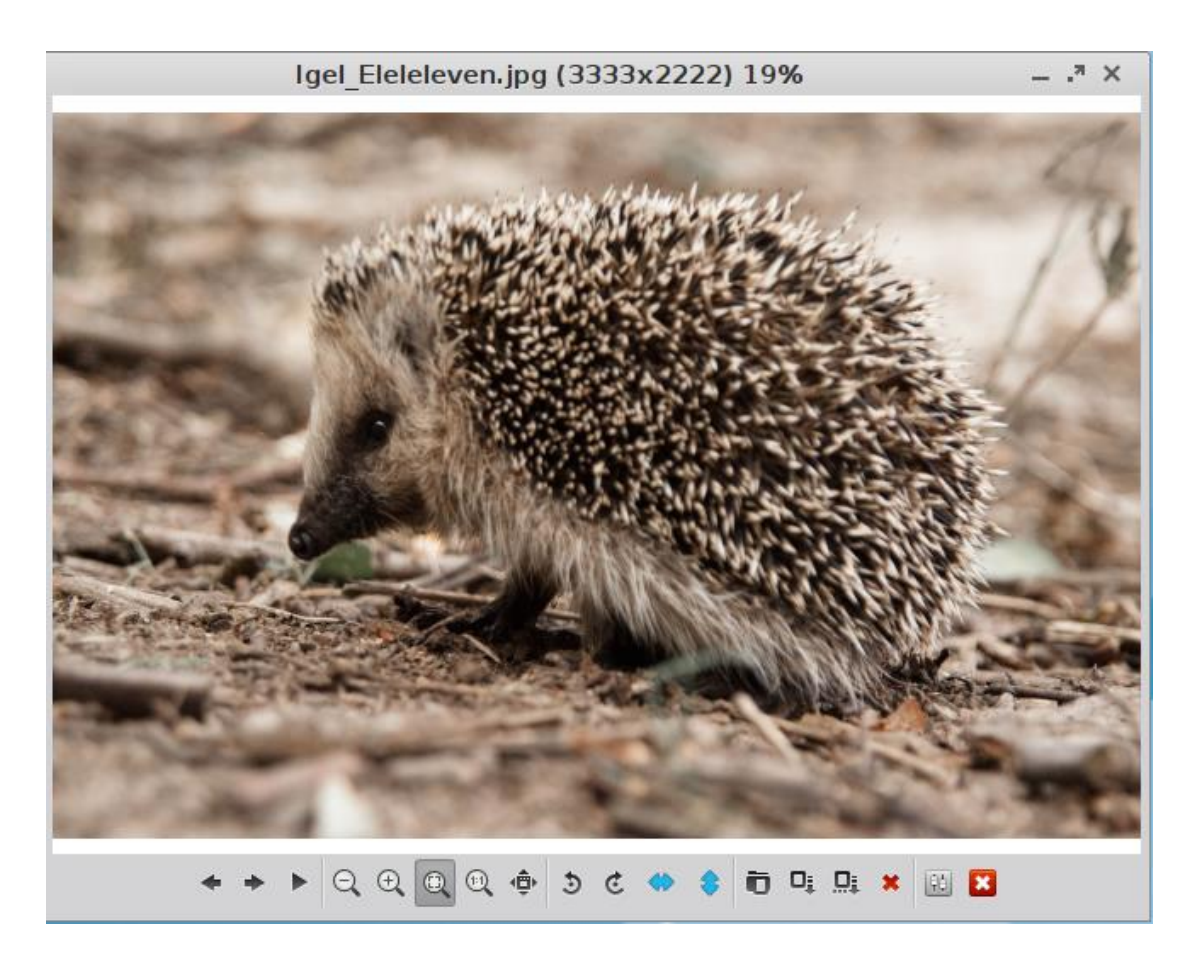


Figure 59: Bildbetrachter

7. Benutzeroberfläche

Gestalten Sie die Benutzeroberfläche ganz nach Ihren Wünschen:

- Legen Sie die *Systemsprache* (Seite 86) fest.
- Gestalten Sie Ihren Bildschirm.
- Definieren Sie *Eingabeoptionen* (Seite 86).
- Erweitern Sie die *Zeichensätze* (Seite 89).

7.1. Bildschirm

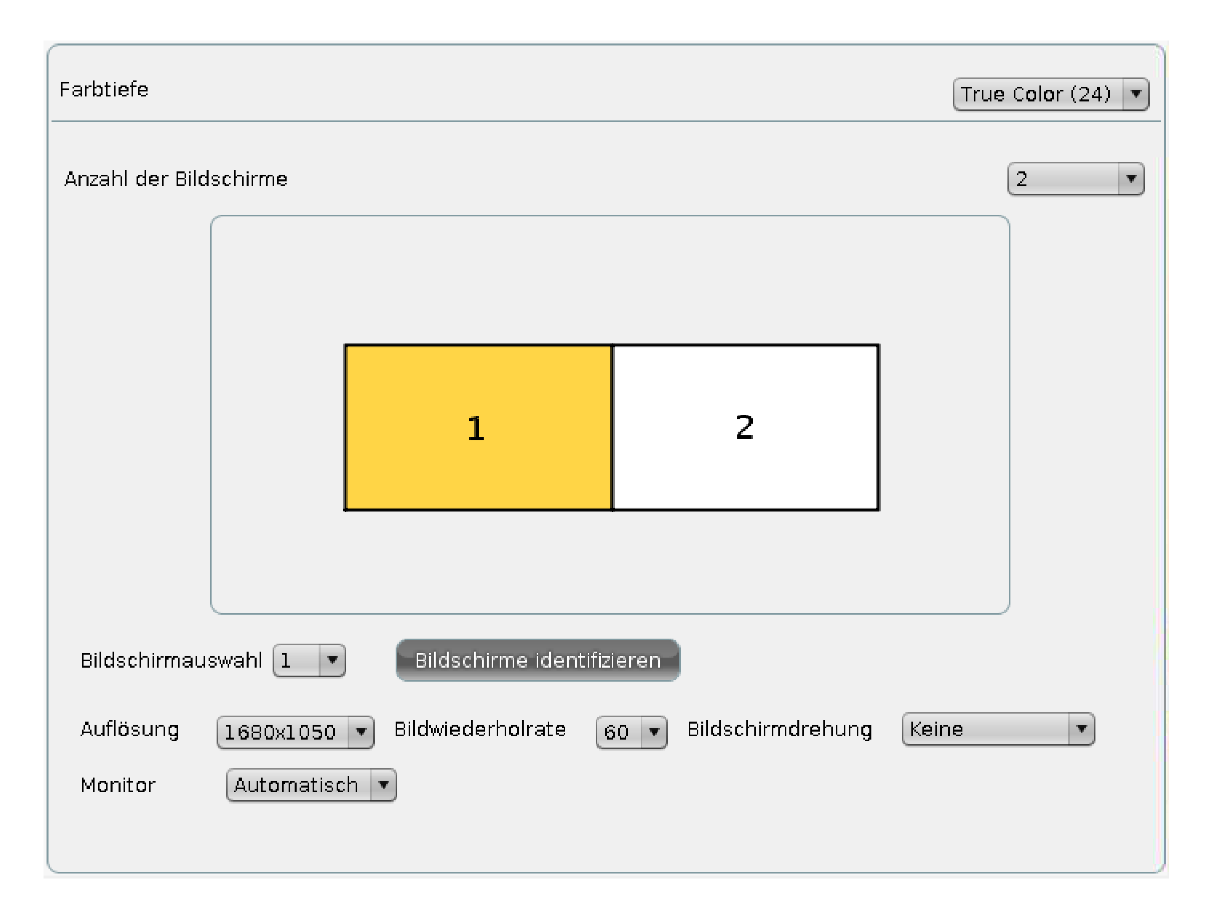


Figure 60: Einstellungen des Bildschirms

Farbtiefe

Auswahl der Arbeitsflächenfarbtiefe - Folgende Optionen stehen zur Verfügung:

- 16 Bit pro Pixel (High Color / 65.000 Farben)
- 24 Bit pro Pixel (True Color / 16,7 Millionen Farben)

> Vergewissern Sie sich, dass alle an den Thin Client angeschlossenen Bildschirme die Farbeinstellung unterstützen.

DDC	Aktivieren des Display Data Channel, um Informationen zwischen System und Bildschirm auszutauschen. Sollten Bildschirmprobleme auftreten, aktivieren und deaktivieren Sie in **Optionen** zum Test die DDC-Einstellung. Standardmäßig ist DDC aktiviert, die vom Bildschirm unterstützte native Auflösung wird automatisch ermittelt.
Bildschirmkonfiguration	Jeder an das IGEL UD-Gerät angeschlossene Bildschirm kann unabhängig konfiguriert werden. Die Position der einzelnen Bildschirme kann in Bezug auf Bildschirm 1 festgelegt werden. Klicken Sie auf **Bildschirme identifizieren**, um die Bildschirmkennung auf jedem Gerät anzuzeigen.

Die von Ihrem IGEL Thin Client unterstützte Bildschirmauflösung entnehmen Sie bitte dem jeweiligen Datenblatt.

Wenn Sie das Feature Shared WorkPlace (SWP) mit benutzerspezifischen Bildschirmauflösungen verwenden, beachten Sie die *Best Practice zum Thema* (*http://edocs.igel.com/index.htm#10202975.htm*).

7.1.1. DPMS

Wenn Ihr Bildschirm Display Power Management Signaling unterstützt, sind weitere Energiesparfunktionen verfügbar. Es werden drei verschiedene Modi angeboten:

- **Standby**,
- **Suspend** (Ruhezustand)
- **Abschalten** (Aus).

Der jeweilige Modus wird nach Ablauf einer einstellbaren Zeitspanne (in Minuten) aktiviert.

Alle Stufen werden natürlich nur dann durchlaufen, wenn der X-Server während dieser Laufzeit keine neuen Eingaben empfängt.

7.1.2. XDMCP

Aktivieren Sie die XDMCP-Funktionalität für den Bildschirm, um den geeigneten Verbindungstyp wählen zu können.

Beachten Sie, dass ein Zugriff auf das lokale Setup dann nur noch über den Hotkey Strg+Alt+s möglich ist, Sie sollten diesen also für die Setupanwendung nicht deaktivieren (**Zubehör→Setup**).

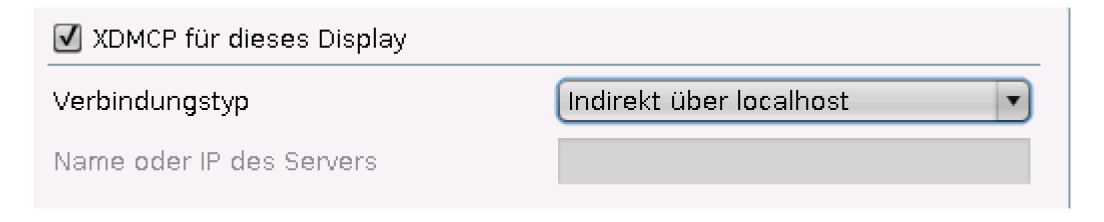


Figure 61: Bildschirm XDMCP

Verbindungstyp	Auswählen des geeigneten Verbindungstyps - Wenn Sie broadcast wählen, wird die grafische Anmeldung vom ersten XDMCP-Server bereitgestellt, der auf die Broadcastanfrage antwortet. Wenn Sie den Verbindungstyp indirekt über localhost auswählen, wird während des Startvorgangs eine Liste mit XDMCP-Hosts angezeigt. Wählen Sie aus dieser Liste den Host aus, der die grafische Anmeldung ausgibt.
Name oder IP des Servers	Dieses Feld ist aktiv, wenn Sie die Verbindungsart direkt oder indirekt wählen. Geben Sie den Namen oder die IP-Adresse des XDMCP-Servers an, den Sie nutzen möchten. Im Modus direkt erhalten Sie die grafische Anmeldemaske direkt vom XDCMP-Server, den Sie im Eingabefeld angegeben haben. Wenn Sie sich für den Modus indirekt entschieden haben, wird eine Liste der verfügbaren XDMCP-Server von dem von Ihnen angegebenen Server bereitgestellt.

> Vergewissern Sie sich, dass der Display-Manager-Dämon (XDM, KMD, GDM ...) ausgeführt wird und dass die Zugangsberechtigung auf dem Remote-Host vorhanden ist.

7.1.3. Zugriffskontrolle

Die **Zugriffskontrolle** des Thin Clients ist standardmäßig aktiviert. Wenn Sie **Konsolenzugriff abschalten** markieren, ist der Zugriff auf Ihren Terminalbildschirm von jedem UNIX-Host aus möglich.

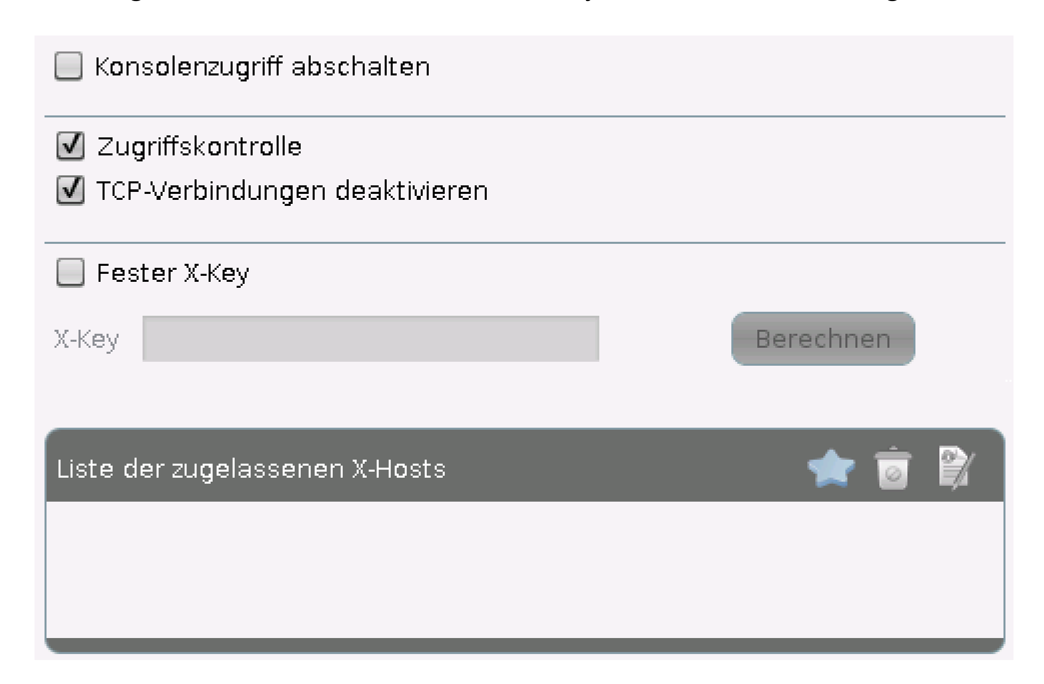


Figure 62: Zugriffskontrolle

Fester X-Key	Sie können für bestimmte Benutzer den permanenten Fernzugriff auf den Thin Client gewähren. Dafür müssen Sie diese Option aktivieren, auf die Schaltfläche **Berechnen** klicken und den erhaltenen 32-stelligen Schlüssel in die Xauthority-Datei auf dem Computer des Benutzers eingeben.
Liste der zugelassenen X Hosts	Klicken Sie auf die Schaltfläche **Hinzufügen**, um die Eingabemaske zu öffnen. Geben Sie den Namen des Remote-Hosts (nicht die IP-Adresse) an, den Sie hinzufügen möchten und bestätigen Sie mit **OK**.

7.1.4. Desktop

Mit Hilfe der folgenden fünf Dialogfelder konfigurieren Sie das Erscheinungsbild und das Verhalten von Arbeitsfläche, Fenstern, Taskleiste, Pager (virtuelle Bildschirme) und Startmenü.

Auf dieser Seite nehmen Sie allgemeine Einstellungen zum Erscheinungsbild des Desktops vor:

- Ändern Sie **Themen der Oberfläche**,
- Bestimmen Sie **Fonts** (Schriftarten)
- Ändern Sie die **Größe der Desktopsymbole**

➢ Konfigurieren Sie die Anzeige- und Verzögerungszeit für **Tooltips**.

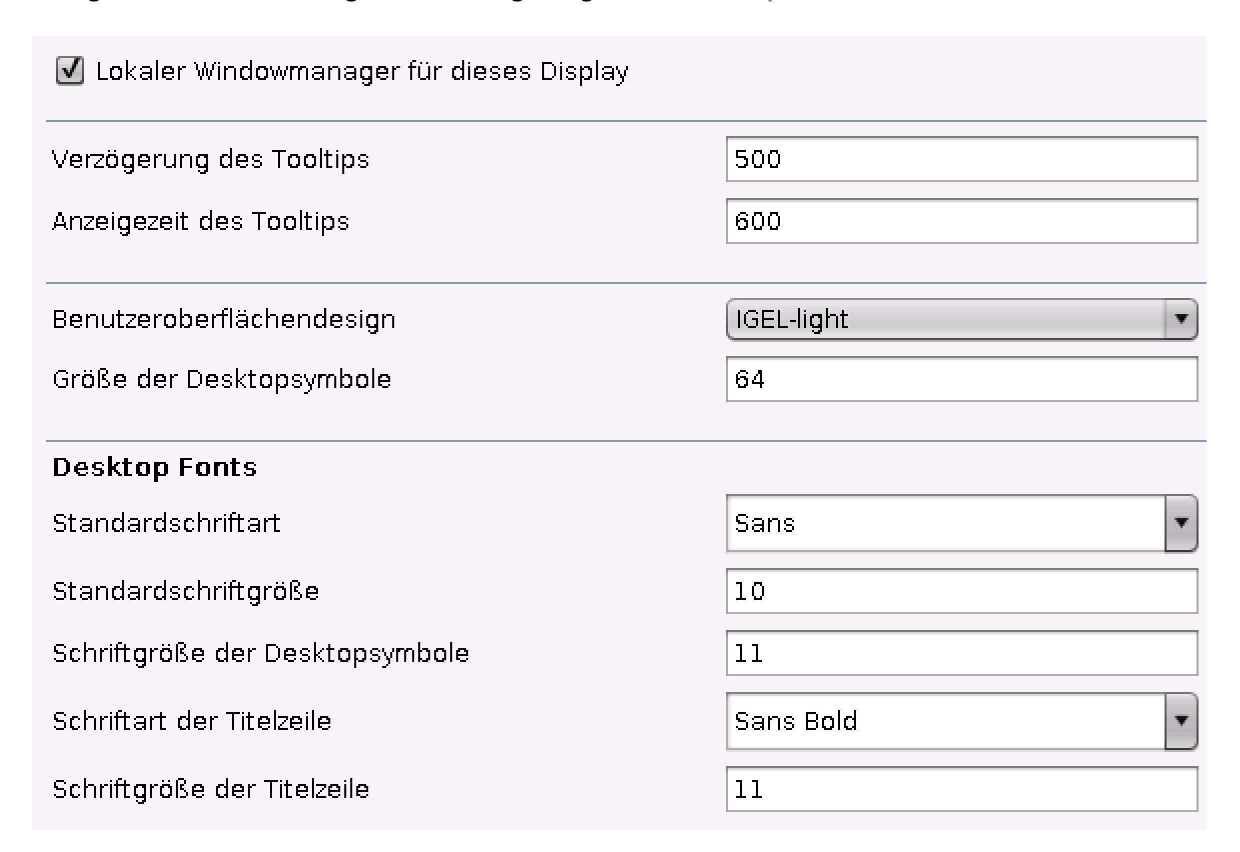
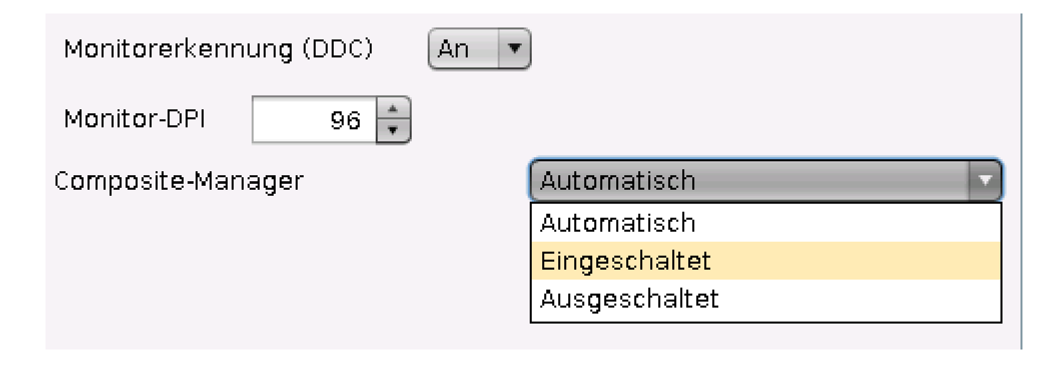


Figure 63: Desktop

7.1.5. Optionen

Konfigurieren Sie hier die Optionen der Bildschirmanzeige:



Monitorerkennung (DDC) Wählen Sie **Aus**, um das automatische Erkennen von Bildschirmeigenschaften auszuschalten.

Monitor-DPI Geben Sie die DPI-Auflösung (Dots Per Inch) ihres Bildschirms ein. Die Voreinstellung ist 96 DPI.

Composite-Manager Hier finden Sie drei Betriebsarten für den Composite-Manager, der Startmenü und Fenster mit Animationen und Effekten ausstattet:

- Automatisch: Deaktiviert den Composite-Manager im Akku-Betrieb, bei gerínger Farbtiefe oder schwacher Hardware
- Eingeschaltet
- Ausgeschaltet

7.1.6. Bildschirmschoner und Bildschirmsperre

Richten Sie den Bildschirmschoner so ein, dass er automatisch nach Ablauf des Zeitlimits, über eine Schaltfläche oder über eine Tastenkombination (**Hotkey**) gestartet wird, und wählen Sie eine Passwortoption. Das Erscheinungsbild der Taskleiste lässt sich für den Anmeldedialog und den gesperrten Bildschirm gesondert konfigurieren.

Beispielkonfiguration einer Bildschirmsperre:

Allgemein

Der Bildschirm lässt sich über Symbole in der Schnellstartleiste und auf dem Desktop oder über den Hotkey Strg-Umschalt-L (Ctrl-Shift-L) sperren.

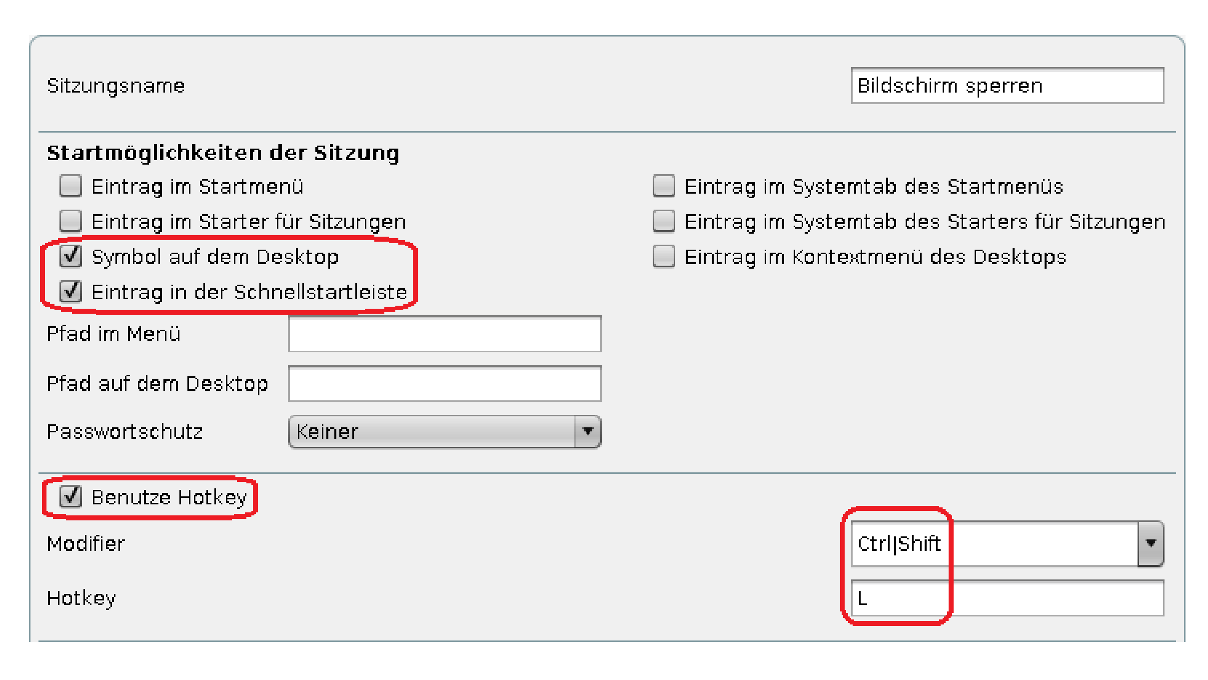


Figure 64: Startoptionen der Bildschirmsperre

Optionen

Die Bildschirmsperre startet automatisch nach 5 Minuten, wenn innerhalb dieses Zeitlimits keine Eingaben am Thin Client erfolgen. Die Sperre kann vom Benutzer oder Administrator mit dem jeweiligen Kennwort aufgehoben werden (siehe: *Passwort* (Seite 114)).

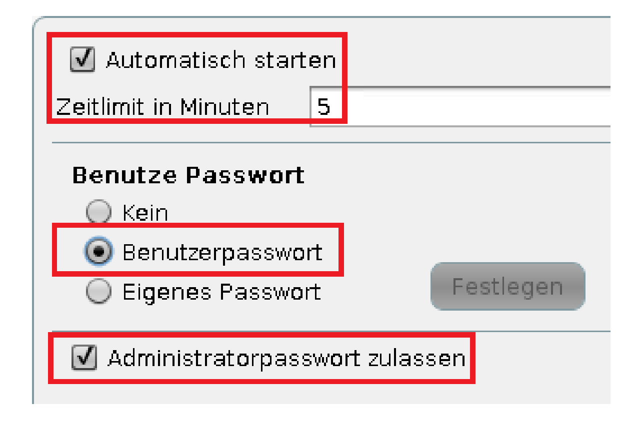


Figure 65: Autostart und Kennwortabfrage

Taskleiste

Für den gesperrten Bildschirm wird keine Taskleiste angezeigt, im Anmeldedialog ist die Taskleiste sichtbar und ermöglicht das Einblenden einer Bildschirmtastatur (z.B. für Touchscreenmonitore).

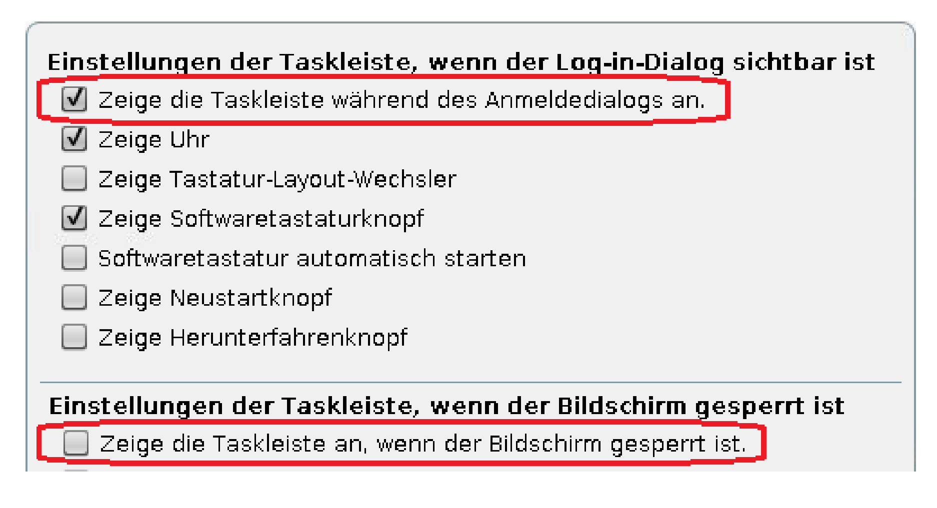


Figure 66: Taskleiste im Anmeldedialog

7.2. Sprache

Wählen Sie aus der Liste die Systemsprache aus. Sie können darüber hinaus die Tastaturbelegung, das Gebietsschema und die Standardformate für Zeit, Währung usw. konfigurieren. Bei der ersten Änderung der Sprache wird die Tastaturbelegung automatisch auf den gleichen Wert gesetzt.

> Die gewählte Sprache ist die Sprache für die Benutzeroberfläche und gilt deshalb für alle lokalen Anwendungen.

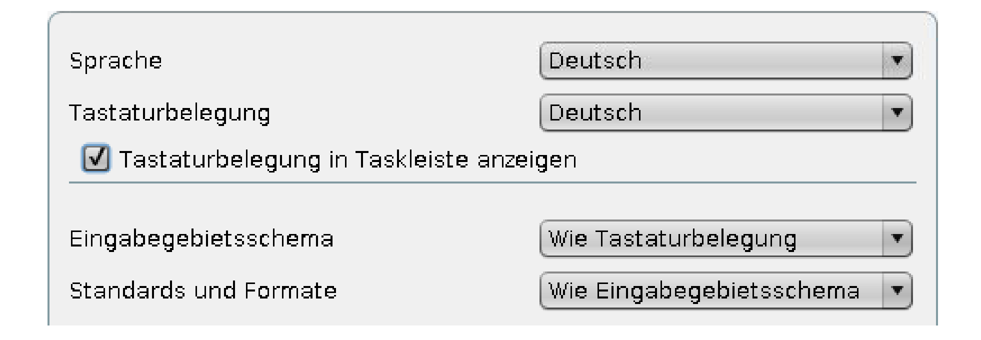


Figure 67: Einstellen der Systemsprache

7.3. Eingabe

Bestimmen Sie auf diesen Setupseiten die Tastaturbelegung und andere Eingabeoptionen.

Folgende Eingabegeräte können eingerichtet werden:

- *Tastatur* (Seite 87)
- *Maus* (Seite 87)
- Touchpad
- *Signaturpad* (Seite 89)

7.3.1. Tastatur und zusätzliche Tastatur

Tastaturbelegung	Festlegen der Tastaturbelegung - Die gewählte Belegung gilt für alle Teile des Systems, einschließlich der Emulationen, Fenstersitzungen und X-Anwendungen.
Tastaturtyp	Festlegen des Tastaturtyps.
Tastenwiederholung	Festlegen des automatischen Wiederholungsverhaltens für die Tastatur: • **Startverzögerung der Tastenwiederholung** – Bestimmt die Verzögerung (in Millisekunden) bis zum Beginn der automatischen Wiederholung. • **Tastenwiederholrate** – Bestimmt die Anzahl der Zeichenwiederholungen pro Sekunde. • **Tottasten aktivieren** – Aktivieren Sie diese Funktion, wenn die verwendete Tastatur Tottasten für Sonderzeichen unterstützt.
Start mit NumLock an	Festlegen, dass **NumLock** während des Startvorgangs automatisch aktiviert werden soll.

➢ Definieren Sie **zusätzliche Tastaturlayouts**, die der Benutzer auswählen kann. Die Belegung kann dann in der Taskleiste ausgewählt oder über konfigurierbare Hotkeys gewechselt werden.

7.3.2. Maus

Linkshändermodus	Ändern der Ausrichtung der Maus durch Vertauschen der Maustasten auf den Linkshändermodus.
Emulation einer 3-Tasten Maus (keine Unterstützung bei serieller Maus)	Aktivieren/deaktivieren der Emulation der dritten (mittleren) Maustaste für Mausgeräte mit nur zwei physischen Tasten - Die dritte Taste wird durch das gleichzeitige Betätigen beider Tasten emuliert. Das Zeitlimit der Emulation bestimmt, wie lange (in Millisekunden) der Treiber wartet, bevor er entscheidet, ob zwei Tasten gleichzeitig gedrückt wurden, wenn die 3-Tasten-Emulation aktiviert wurde.
Mausgeschwindigkeit	Bestimmen der Auflösung der Maus in Zählern pro Zoll
Maus Doppelklick Intervall	Verändern des maximalen Intervalls (in Millisekunden) zwischen zwei aufeinander folgenden Mausklicks, die als Doppelklick erkannt werden sollen.
Mauszeiger ausblenden	Nach Ablauf des definierten Zeitlimits wird der Mauszeiger ausgeblendet.

7.3.3. Touchscreen

Die Erstkonfiguration sollte mit angeschlossener Maus und Tastatur erfolgen, damit Sie das Setup öffnen und darin navigieren zu können. Das Setup mit Bildschirmtastatur wird im Folgenden beschrieben.

Touchscreentreiber	Die derzeit unterstützten Touchscreentypen sind: • Elographics-Seriell-Touchscreens • TSharc-Seriell-Touchscreens • EvTouch-USB-Touchscreens Die komplette Liste der unterstützten Geräte finden Sie in der *IGEL Hardware Datenbank* (*https://www.igel.com/service-support/linux-3rd-party-hardware-database.html*).
Touchscreen ist bereits kalibriert	Nach dem Aktivieren der Touchscreenfunktion muss sie zunächst kalibriert werden. Wenn diese Option nicht aktiviert wurde, startet die Kalibrierung automatisch nach jedem Systemstart.
X- und Y-Werte vertauschen	Aktivieren Sie diese Option, wenn sich beim Bewegen des Fingers in horizontaler Richtung der Mauszeiger in vertikaler Richtung bewegt.
Minimaler/maximaler X-Wert/Y-Wert	Diese Werte werden vom Kalibrierungstool festgelegt. Sie können sie jedoch auch manuell verändern.
Loslasslimit	Maximal zulässige Zeit (in Millisekunden) zwischen zwei Berührungsaktionen, um noch als einzelne Berührung registriert zu werden. So kann beispielsweise beim Bewegen von Fenstern per Drag-and-Drop die Berührung unbeabsichtigt unterbrochen werden. Das Erhöhen dieses Werts verhindert, dass der Thin Client dieses Loslassen als zwei einzelne Berührungen wertet.
Berührungslimit	Bestimmen, wie lange (in Millisekunden) der Touchscreen berührt werden muss, damit die Berührung erkannt wird.
Baudrate (nur bei seriellen Touchscreens)	Festlegen der Kommunikationsgeschwindigkeit über den ausgewählten Anschluss. (Im Zweifel lesen Sie das Monitorhandbuch.)
Touchscreenanschluss	Sie können den Touchscreen entweder an COM1 oder COM2 anschließen. Wählen Sie den gewünschten Anschluss hier aus.
Treiberspezifische Standardeinstellungen festlegen	Klicken Sie einmal auf diese Schaltfläche, nachdem Sie den Touchscreentyp geändert haben oder um die Standardeinstellungen wiederherzustellen.

Eine Liste der zur Zeit von IGEL Linux unterstützen Touchscreens finden Sie auf www.igel.de.

➢ Aktivieren Sie die Bildschirmtastatur für die Touchscreennutzung im Setup unter **Zubehör→Bildschirmtastatur.**

Die Belegung der normalen Tastatur wird auch für die Bildschirmtastatur verwendet.

Kalibrieren Sie den Touchscreen für eine optimale Erkennung der Berührung. Das Anwendung Touchscreen Kalibrierung finden Sie im **Starter für Sitzungen→System**.

Nachdem das Kalibrierungsprogramm gestartet wurde, wird ein Muster mit Kalibrierungspunkten angezeigt, die nacheinander berührt werden müssen.

7.3.4. SCIM Eingabemethoden

Die Smart Common Input Method (SCIM) Plattform bietet Eingabemethoden unter Linux für über 30 Sprachen.

- Aktivieren Sie eine der vom IGEL System bereitgestellten Methoden (Chewing und Smart Pinyin) oder verwalten Sie generische Tabellen zur Beschreibung der Eingabemethode.

7.3.5. Signaturpad

Aktivieren Sie den **StepOver TCP Client**, um USB-Signaturpads des Herstellers StepOver in Sitzungen verwenden zu können.

> Detaillierte Hinweise zur Konfiguration von Signaturpads finden Sie in Best Practices zu StepOver Pads und Softpro/Kofax Pads.

7.4. Tastaturbefehle - Hotkeys

Hier finden Sie eine Liste der bestehenden **Tastaturbefehle** zur Fenstersteuerung. Für jede Funktion kann eine Tastenkombination definiert werden.

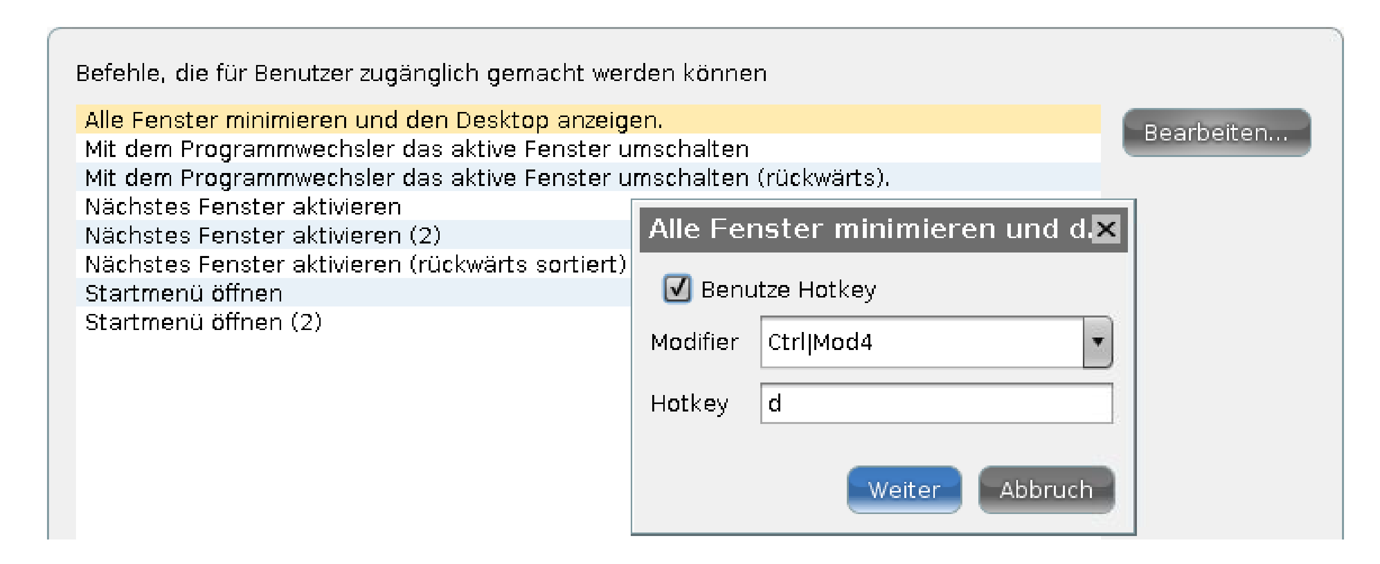


Figure 68: Tastaturbefehle

7.5. Fontservices

Sie können zusätzlich zu den von IGEL bereitgestellten Zeichensätzen noch weitere importieren:

- *XC-Fontservice* (Seite 90)
- *NFS-Fontservice* (Seite 90)

7.5.1. XC-Fontservice

Wenn Sie neben den vom Thin Client bereitgestellten Zeichensätzen (Fonts) weitere Zeichensätze benötigen, können Sie den XC-Fontservice nutzen.

Dieser Service muss auf dem Server installiert und komplett dort konfiguriert werden.

Der Vorteil der Nutzung des XC-Fontservices im Vergleich zu NFS ist die bessere Performance.

➢ Klicken Sie **XC-Fontservice aktivieren**, um die folgenden Eingabefelder zu aktivieren.

XC-Fontserver	Geben Sie den Server an, auf dem der XC-Fontservice ausgeführt wird.
Portnummer	Geben Sie die Portnummer an, auf dem der Fontservice empfängt - Standardeinstellung ist Portnummer 710.
Lokale Fonts bevorzugen	Aktivieren Sie diese Option, wenn lokale Zeichensätze verwendet werden sollen, bevor eine Anfrage an den Fontserver gesendet wird.

7.5.2. NFS-Fontservice

Eine weitere Möglichkeit, zusätzliche Zeichensätze zu importieren, ist die Nutzung des NFS-Fontservice. Der NFS-Fontservice bietet zusätzlich den Vorteil, dass der Einhängepunkt für die Zeichensätze konfiguriert werden kann. Dies ist für einige Remote-Anwendungen erforderlich, die in einem bestimmten Verzeichnis nach ihren Zeichensätzen suchen.

➢ Definieren und aktivieren Sie einen NFS-Font-Path-Eintrag, um den NFS-Fontservice zu verwenden.

Dieser wird zur **Liste der NFS gemounteten Schriftartenverzeichnisse** hinzugefügt.

➢ Klicken Sie auf **Hinzufügen**, um das Dialogfenster zu öffnen:

Lokales Verzeichnis	Festlegen des lokalen Verzeichnisses für den Einhängepunkt
NFS-Server	Namen oder IP-Adresse des Servers, der über NFS die Zeichensatzverzeichnisse zur Verfügung stellt.
Serverpfad	Pfad auf dem Server, unter dem die Zeichensätze verfügbar sind.
Lokale Fonts bevorzugen	Ist diese Option aktiviert, werden lokale Zeichensätze verwendet, bevor eine Anfrage an den Fontserver gesendet wird.

➢ Klicken Sie **Aktivieren**, um den Eintrag zu aktivieren.

➢ Exportieren Sie das Zeichensatzverzeichnis über NFS-Read-only für den Thin Client auf den Server.

8. Netzwerk

Konfigurieren Sie die Netzwerkverbindungen des Thin Clients:

- *LAN-Schnittstellen* (Seite 91)
- *Drahtlosverbindungen (WLAN)* (Seite 96)
- *DHCP-Optionen*
- *Virtual Privat Network (VPN)*
- *Zertifikatsverwaltung mit SCEP*
- *Netzwerkroute*
- *Hosts*
- *Netzlaufwerke* (Seite 103)
- *Systemweiter Proxy* (Seite 105)

8.1. LAN-Schnittstellen

➢ Klicken Sie im Setup des Clients **Netzwerk→LAN-Schnittstellen**.

➢ Wählen Sie zwischen dem automatischen Netzwerksetup mit den Protokollen DHCP und BOOTP oder der manuellen Netzwerkkonfiguration um den Thin Client für jede Netzwerkschnittstelle einzustellen.

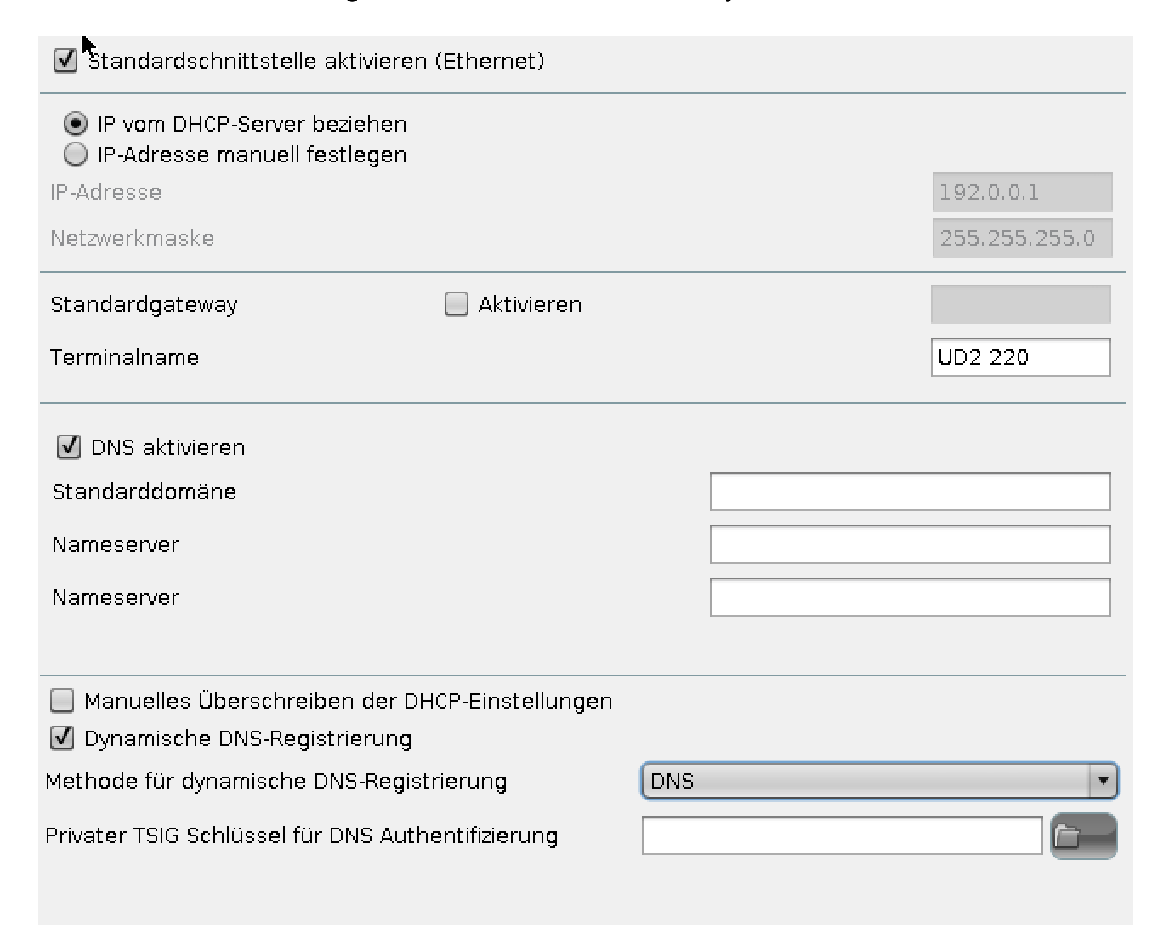


Figure 69: LAN-Schnittstellen

DHCP	Über das Dynamic Host Configuration Protocol empfängt der Thin Client seine IP-Adresse, Netzwerkmaske, DNS, Gateway und andere Netzwerkkonfigurationen von einem DHCP-Server. DHCP ist standardmäßig aktiv für LAN 1 (intern). DHCP-Optionen lassen sich im Menü **DHCP Client** aktivieren, dabei steht eine Liste von Standardoptionen zur Verfügung, es können aber auch eigene Optionen definiert werden.
BOOTP	Über das **BOOTP** empfängt der Thin Client die IP-Adresse, Netzwerkmaske, DNS, das Gateway und andere Netzwerkkonfigurationen von einer BOOTP-Serverdatenbank.

> Die Übertragung einer `setup.ini`-Datei oder eines Bootskripts wird nicht unterstützt. BOOTP wird nicht verwendet, um ein Bootimage von einem Server abzurufen und dieses Image zu booten, wie die Bezeichnung BOOTP vermuten lässt.

IP-Adresse manuell festlegen	Manuelles Vornehmen der Netzwerkeinstellungen, anstatt nach einem DHCP-Server zu suchen - Vergewissern Sie sich, dass die feste IP-Adresse, die Sie eingeben, nicht von einem anderen Computer in Ihrem Netzwerk verwendet wird. Wenn Sie ein Gateway nutzen müssen, um die Datenpakete zu und aus dem Zielnetzwerk weiterzuleiten, klicken Sie auf **aktivieren**, und geben Sie die Gateway-IP-Adresse ein.
Terminalname	Geben Sie den lokalen Namen des Thin Clients an. Ansonsten wird der Standardname IGEL <MAC-Adresse> generiert.
DNS aktivieren	Konfigurieren des DNS - Legen Sie die **Standard Domain**, in der das Gerät arbeiten soll, sowie die IP-Adresse von bis zu zwei **Namensservern** fest, die nacheinander abgefragt werden.
Manuelles Überschreiben der DNS-Einstellungen	Manuelle Einträge überschreiben die Standardroute, den Domänennamen und die DNS-Server.
Dynamische DNS-Registirierung	Hier haben Sie die Möglchkeit, die aktuelle IP-Adresse des Thin Clients automatisch an das DNS zu melden. Es stehen die Methoden **DHCP** und **DNS** zur Verfügung. Wählen Sie **DNS**, müssen Sie unter Umständen einen **privaten TSIG-Schlüssel für die DNS-Authentifizierung** angeben.

> Eine Anleitung für die Dynamische DNS-Registrierung per DNS gibt ein *FAQ-Dokument http://edocs.igel.com/index.htm#10203508.htm*.

8.1.1. Einzelne Schnittstelle

Unter dem Namen der einzelne Schnittstelle (beispielsweise Schnittstelle 1) können Sie einige der allgemeinen Einstellungen für Lan-Schnittstellen überschreiben. Daneben gibt es zwei weitere Einstellungen:

IPv6-Konfiguration Hier wählen Sie eine Konfigurationsart für den Betrieb mit IPv6. Näheres erklärt ein *Best-Practice Dokument* *http://edocs.igel.com/index.htm#10203497.htm*.

Netzwerklinktyp Geben Sie den Netzwerklinktyp der Schnittstelle an. Standard ist **Automatische Erkennung**.

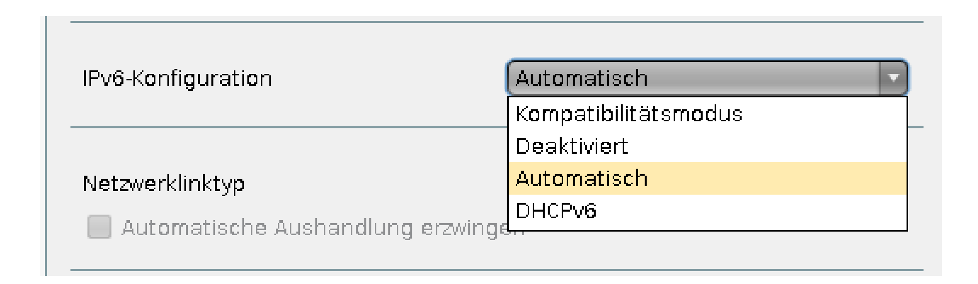


Figure 70: Konfiguration einer einzelnen LAN-Schnittstelle

8.1.2. Authentifizierung

IEEE 802.1x Authentifizierung aktivieren (nur Wired 802.1x) Aktivieren der Netzwerkport-Authentifizierung gemäß dem 802.1x-Standard. Derzeit werden die folgenden Authentifizierungsmethoden unterstützt:

- EAP-PEAP/MSCHAPv2
- EAP-PEAP/TLS
- EAP-TLS

> Die Eingabeoptionen im Menü **Authentifizierung** ändern sich je nach der gewählten Authentifizierungsmethode. Werden die Felder **Kennung** und **Passwort** nicht vorbelegt, wird zur Authentifizierung eine Eingabemaske angezeigt.

EAP-Typ	Wählen der Authentifizierungsmethode: • PEAP für EAP-PEAP/MSCHAPv2 und EAP-PEAP/TLS • TLS für EAP-TLS
Serverzertifikat prüfen	Prüfen des Authentifizierungsservers
CA-Stammzertifikat	Pfadname der Datei mit Root-Zertifikat(en) zur Serverauthentifizierung. Die Datei kann im PEM- oder DER-Format vorliegen.
PEAP/Auth Methode	Wählen Sie die Phase-2-Authentifizierungsmethode • MSCHAPv2 für EAP-PEAP/MSCHAPv2 • TLS für EAP-PEAP/TLS.
EAP-PEAP/MSCHAPv2/Kennung	Benutzernamen zur Anmeldung für MSCHAPv2-Authentifizierung beibehalten.
EAP-PEAP/MSCHAPv2/Passwort	Passwort für MSCHAPv2-Authentifizierung beibehalten.
EAP-PEAP/TLS/Clientzertifikat	Pfadname der Datei mit dem Zertifikat zur Clientauthentifizierung im PEM- (base64) oder DER-Format. Freilassen, falls privater Schlüssel im PKCS12 Format benutzt wird.
EAP-PEAP/TLS/Privater Schlüssel	Eingeben des Pfadnamens der Datei mit dem privaten Schlüssel des Clientzertifikats im PEM- (base64), DER- oder PFX-Format
EAP-PEAP/TLS/Kennung	Benutzername zur Anmeldung für die TLS-Authentifizierung
EAP-PEAP/TLS/Passwort für privaten Schlüssel	Passwort für den Zugriff auf den verschlüsselten privaten Schlüssel in der privaten Schlüsseldatei
EAP-TLS/Clientzertifikat	Pfadname der Datei mit dem Zertifikat zur Clientauthentifizierung im PEM- (base64) oder DER-Format; freilassen, falls privater Schlüssel im PKCS12 Format benutzt wird.
EAP-TLS/Privater Schlüssel	Pfadname der Datei mit privatem Schlüssel des Clientzertifikats im PEM- (base64), DER- oder PFX-Format
EAP-TLS/Kennung	Benutzername zur Anmeldung für die TLS-Authentifizierung
EAP-TLS/Passwort für privaten Schlüssel	Passwort für den Zugriff auf den verschlüsselten privaten Schlüssel in der privaten Schlüsseldatei.

Für die Authentifizierung per IEEE 802.1x lässt sich das Clientzertifikat auch über SCEP anfordern und verwalten. Siehe *Netzwerk/SCEP* (Seite 101).

8.1.3. Wake-on-LAN

Wählen Sie aus, mit welchen Paketen bzw. Nachrichten der Thin Client über das Netzwerk gestartet werden kann:

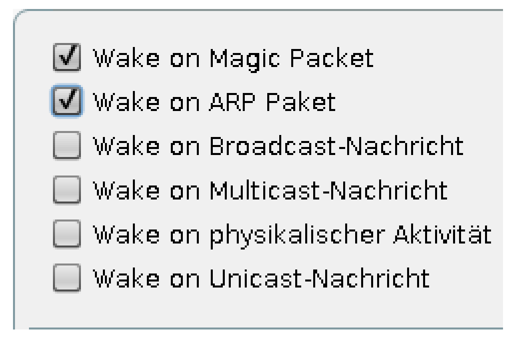


Figure 71: Wake-on-LAN Optionen

8.2. WLAN

In diesem Bereich konfigurieren Sie alles rund um Ihre WLAN-Verbindungen.

Kompatible WLAN-Module finden Sie in unserer *IGEL Linux 3rd Party Hardware Datenbank* (*https://www.igel.com/service-support/linux-3rd-party-hardware-database.html*).

Wenn Sie mobile Geräte verwenden und sich öfter in wechselnden WLAN-Bereichen aufhalten, profitieren Sie von unserer neuen Funktionalität: IGEL Café Wireless. Das heißt, Sie können wie Sie es auch von Smartphones her kennen, direkt von der Benutzeroberfläche aus über den WiFi-Manager

- sich einfach in neue, bisher unbekannte WLAN-Netze verbinden,
- einmal angelegte Verbindungen speichern und später wiederverwenden.

Bei stationären Desktopgeräten, die zentral verwaltet werden, hat diese Funktionalität keine Bedeutung. Hier geht man von einem fest eingestellten Netz aus, das der Endbenutzer nicht beeinflussen soll.

So konfigurieren Sie die WLAN-Schnittstelle:

1. Öffnen Sie das **IGEL Setup** und klicken Sie **Netzwerk→LAN-Schnittstellen→WLAN**.

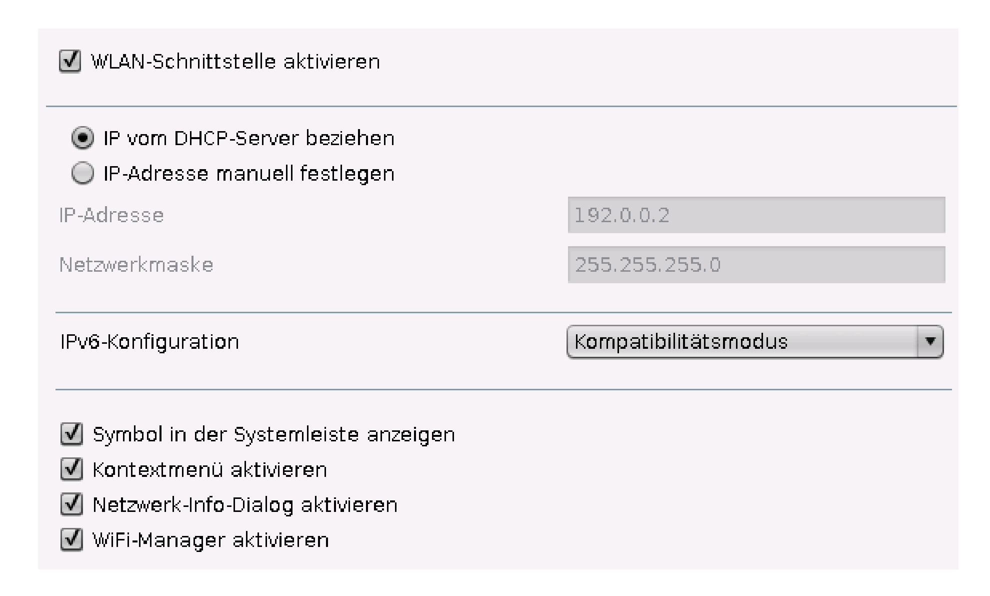


Figure 72: Benutzerdefinierte Verbindungen aktivieren

2. Aktivieren Sie die **WLAN-Schnittstelle**.
3. Wählen Sie die Konfiguration Ihrer **IP-Adressen** (DHCP oder manuell vergeben).
4. Wählen Sie eine Konfigurationsart für den Betrieb mit **IPv6**.
5. Aktivieren Sie zumindest die Elemente **Systemleistensymbol**, **Kontextmenü** und **WiFi-Manager**. Über den WiFi-Manager können Sie IGEL Café Wireless nutzen.

   Stellen Sie sicher, dass der Parameter **Sitzungen überschreiben** inaktiv ist für UMS-Profile mit dieser WLAN-Konfiguration. Andernfalls werden benutzerdefinierte Verbindungen beim Neustart des Thin Clients verloren gehen.

6. Konfigurieren Sie die drahtlose Netzwerkverbindung im Dialog Standard-WLAN, wenn Sie sie nicht über den WiFi-Manager auswählen.

   Zusätzliche Verbindungen lassen sich im Dialog Weitere WLANs konfigurieren.
7. Konfigurieren Sie Ihren Standort im Dialog WLAN-Frequenzbereiche.

Nachdem diese Einstellungen auf dem Thin Client aktiv geworden sind, erscheint ein neues Symbol für Drahtlosverbindungen in der Systemleiste:

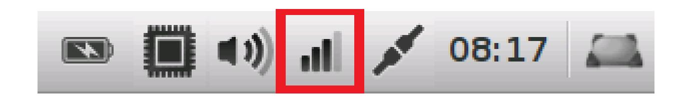


Figure 73: WiFi-Symbol

8.3. DHCP-Client Optionen

Konfigurieren Sie die clientseitige Verwendung von DHCP-Optionen - einige **Standardoptionen** sind bereits in einer Liste aufgeführt und können aktiviert werden. **Benutzerdefinierte Optionen** lassen sich in einer eigenen Listen anlegen und verwalten.

8.4. Virtual Private Network - VPN

Über Virtual-Private-Network-Protokolle (VPN) greifen Remote-Benutzer sicher auf Unternehmensnetzwerke zu. Richten Sie Ihren Client entsprechend dafür ein.

8.4.1. PPTP

PPTP (Point-to-Point Tunneling Protocol) ist eines der gebräuchlichsten Virtual-Private-Network-Protokolle (VPN), mit denen Remote-Benutzer sicher auf Unternehmensnetzwerke zugreifen.

Automatischer Verbindungsaufbau während Bootvorgang

Um einen komplett für den automatischen Verbindungsaufbau konfigurierten Client einzurichten, müssen Sie sich möglicherweise zunächst einwählen.

1. Aktivieren Sie die Option **Automatischer Verbindungsaufbau während Bootvorgang**
2. Klicken Sie auf **Hinzufügen**, um neue Verbindungen einzurichten.
3. Nehmen Sie die erforderlichen Einstellungen vor, um sich am RAS-Server auf der gewünschten Remote-Station einzuwählen.
4. Wählen Sie das Netzwerkgerät und geben Sie an, ob eine Einwahlverbindung verwendet werden soll.
5. Bestimmen Sie auf der Registerkarte **Optionen** den Namenservice und die IP-Konfiguration für die PPTP-Verbindung.

   > Üblicherweise werden diese Daten vom RAS-Server der Remote-Station übermittelt, sodass standardmäßig sowohl DNS als auch IP-Adresse auf **automatisch** gesetzt sind.

Auf den weiteren drei Setupseiten (Routing) können Sie zusätzliche Netzwerkstrecken einrichten.

8.4.2. OpenVPN

Der OpenVPN-Client setzt ein virtuelles privates Netzwerk mittels TLS-Verschlüsselung um und benötigt OpenVPN 2.x als VPN-Server.

Er unterstützt folgende Authentifizierungsmethoden:

- TLS-Zertifikate
- Name/Passwort
- Name/Passwort und Zertifikate
- Statischer Schlüssel

➢ Klicken Sie das Stern-Symbol, um eine neue OpenVPN-Verbindung anzulegen.

Wie Sie OpenVPN-Verbindungen einrichten beschreibt ein *Best-Practice-Dokument* *http://edocs.igel.com/index.htm#10203430.htm*.

8.4.3. GeNUCard

Die VPN-Hardware GeNUCard stellt vorkonfigurierte Internet- und VPN-Verbindungen zur Auswahl.

Das Auswahlfenster öffnet sich unmittelbar nach dem Start der GeNUCard-Sitzung. Die verfügbaren Startoptionen der Sitzung lassen sich in der Sitzungskonfiguration unter **Arbeitsflächenintegration** festlegen.

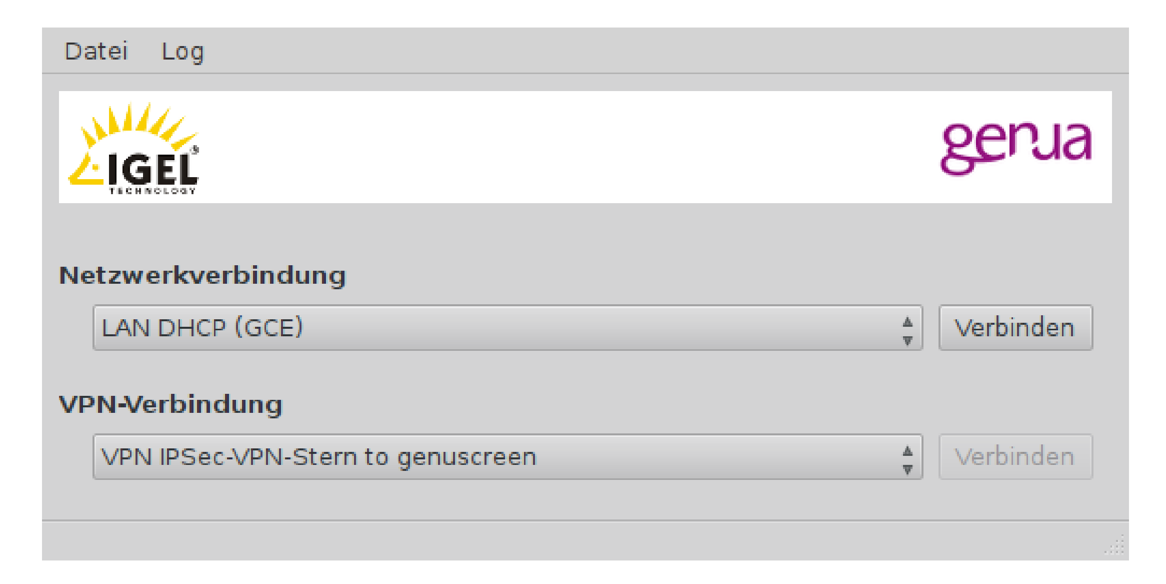


Figure 74: GeNUCard Konfiguration

Unter dem Menü **Datei** finden sich die Einträge für **PIN ändern** sowie **Neuen Schlüssel generieren**.

Optionen

Eine gültige Kombination aus Verbindungs- und Benutzerdaten kann im IGEL Setup vorbelegt werden: **Netzwerk→VPN→GeNUCard→Optionen**.

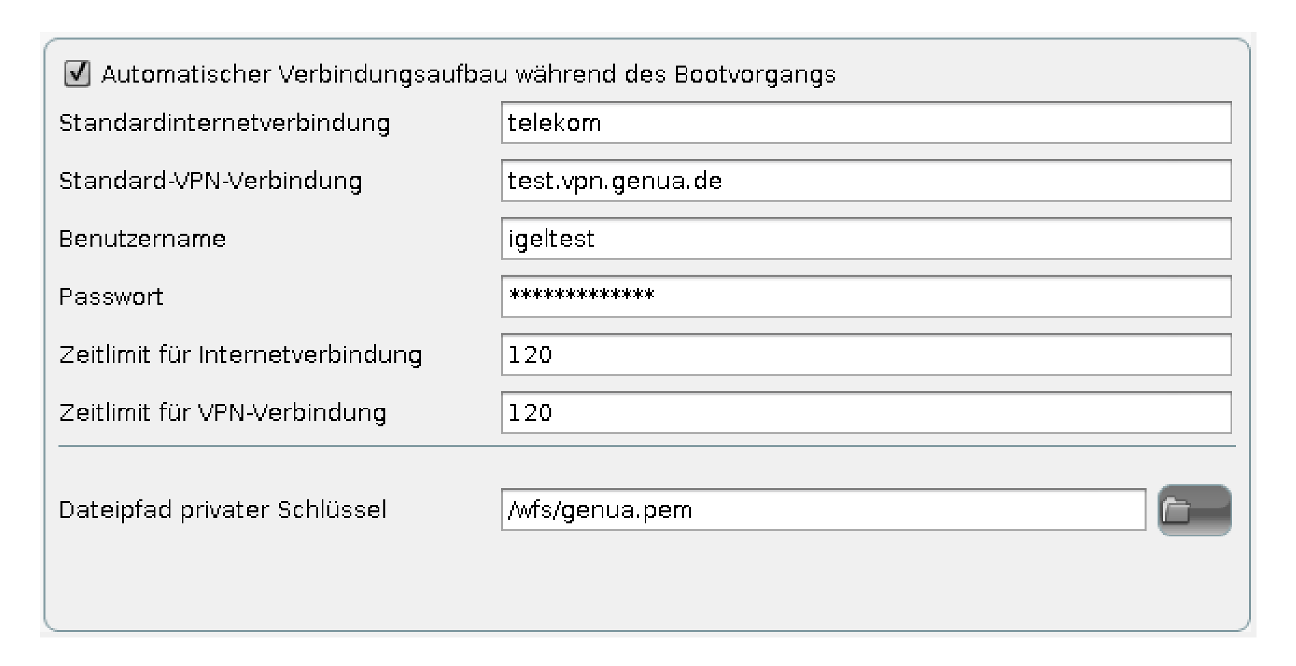


Figure 75: Automatischer Verbindungsaufbau

Auch der automatische Verbindungsaufbau während des Bootvorgangs kann aktiviert werden. Dies ist z. B. notwendig für die Aktualisierung der IGEL Firmware über das VPN.

Administrator Session

Die Konfiguration und Administration der GeNUCard erfolgen zentral über die Management Station genucenter. Weitere Informationen erhalten Sie unter www.genua.de.

Optional lässt sich eine Administratorsitzung erstellen, mit welcher die Internetverbindung der GeNUCard konfiguriert werden kann:

1. Klicken Sie **Instanz hinzufügen** unter **System→Registry→genucard%**.

   Das GeNUCard-Icon erscheint auf der Arbeitsfläche.

2. Klicken Sie das GeNUCard-Icon.

   Das GeNUCard-Anmeldefenster öffnet sich.

3. Geben Sie **Benutzername** und **Passwort** ein.
4. Klicken Sie **Anmelden**.

Das Internet/VPN-Fenster öffnet sich.



Figure 76: Internet/VPN-Fenster

5. Konfigurieren Sie im Bereich **Internet** die Verbindung mithilfe der Schaltflächen **Erstellen**, **Bearbeiten**, **Löschen**.

8.4.4. NCP

Konfigurationsparameter des NCP-Client werden ausschließlich über die Programmoberfläche des Clients selbst konfiguriert.

Die Dokumentation zum NCP Secure Enterprise-Client finden Sie unter:

http://www.ncp-e.com/de/support/produktunterlagen/handbuecher.html

8.5. Simple Certificate Enrollment Protocol - SCEP

SCEP erlaubt die automatische Bereitstellung von Clientzertifikaten über einen SCEP-Server und eine Zertifizierungsstelle. Ein solches Zertifikat wird vor Ablauf der Gültigkeit automatisch erneuert und kann etwa für die Netzwerkauthentifizierung verwendet werden (IEEE 802.1x z.B.).

Als Gegenstelle (SCEP-Server und Zertifizierungsstelle) kann z. B. ein Microsoft Windows 2008 Server dienen (MSCEP, NDES), mehr Information dazu finden Sie bei Microsoft z. B. im Whitepaper.

http://download.microsoft.com/download/a/d/f/adf2dba9-92db-4765-bf2d-34b1c8df9ca3/Microsoft%20SCEP%20implementation%20whitepaper.doc

- Aktivieren Sie die Zertifikatsverwaltung per **SCEP Client** (NDES) und nehmen Sie anschließend die notwendigen Konfigurationen vor.

Nähere Informationen zu SCEP finden Sie auch in der *IGEL Knowledge Base http://edocs.igel.com/*.

8.5.1. Zertifikat

➢ Bestimmen Sie unter **Zertifikat** die Grunddaten des von der Zertifizierungsstelle auszustellenden Zertifikats.

Typ des CommonName	Für ein Clientzertifikat des Thin Clients bietet sich der Typ DNS Name (auto) an, falls der Client seinen Netzwerknamen automatisch bezieht.
Organisationseinheit	Wird von der Zertifizierungsstelle vorgegeben.
Organisation	Frei definierbare Bezeichnung der Organisation, welcher der Client angehört.
Ort, Bundesland, Land	Geben Sie die örtliche Zuordnung des Clients an.
RSA-Schlüssellänge	Wählen Sie eine (von der Zertifizierungsstelle verwendbare) Schlüssellänge für das auszustellende Zertifikat.

8.5.2. Zertifizierungsstelle

➢ Tragen Sie den Namen der Zertifizierungsstelle und den Hashwert des Rootzertifikats ein.

Beides erhalten Sie von der Zertifizierungsstelle.

8.5.3. SCEP-Server

Neben der Zertifizierungsstelle muss auch ein SCEP-Server definiert werden.

➢ Geben Sie **Adresse** und **Anfragepasswort** des SCEP-Servers ein.

Das Passwort generiert der SCEP-Server als Einmalpasswort. Es wird für die erstmalige Anforderung eines Zertifikats benötigt. Neue Zertifikate werden vor Ablauf des alten angefordert, wobei das noch gültige Zertifikat dabei als Authentifizierung dient.

➢ Definieren Sie für die Prüfung der Gültigkeit ein **Intervall** (Häufigkeit der Prüfung) und einen **Zeitraum**, in dem die Zertifikatserneuerung stattfinden muss.

Beispiel:

Ein Zertifikat ist bis zum 31.12. eines Jahres gültig. Der Zeitraum für die Erneuerung beträgt 10 Tage. Dann wird erstmalig am 21.12. desselben Jahres ein neues Zertifikat angefordert.

Durch die Notwendigkeit der Eingabe von Fingerabdruck (Root-Zertifikat der Zertifizierungsstelle) und Anfragepasswort (SCEP Server) ist die Konfiguration etwas „sperrig" und wird idealerweise im UMS als

Profil angelegt und an die Clients verteilt. Dabei kann das Zertifikat noch nicht für die Kommunikation verwendet werden.

8.5.4. Prüfung des Clientzertifikats

Wurde vom SCEP-Server ein Zertifikat der Zertifizierungsstelle an den Client weitergeleitet, wird es dort im Verzeichnis `/wfs/scep_certificates` abgelegt.

Mit dem Shell-Kommando `cert_show_status` können Sie sich die Daten (z. B. die Gültigkeit, das Erstellungsdatum und den Hashwert) des Zertifikats anzeigen lassen.

8.5.5. Anwendungsbeispiel

Per SCEP ausgestellte und verwaltete Zertifikate können z. B. für die Netzwerkauthentifizierung verwendet werden.

Entsprechende Optionen finden Sie in der Konfiguration der IEEE 802.1x Authentifizierung

Netzwerk→LAN-Schnittstellen→Schnittstelle 1→Authentifizierung

oder auch bei der Einrichtung des drahtlosen Netzwerks

Netzwerk→LAN-Schnittstellen→Wireless→Authentifizierung, Verschlüsselung WPA Enterprise, EAP Typ TLS.

Ein Problem bei der Verteilung des Clientzertifikats per Netzwerk ist, dass dieses Zertifikat für die Kommunikation benötigt wird. Die Verwendung von SCEP in Verbindung mit 802.1x Authentifizierung ist insofern unproblematisch, als die Erstanforderung des Clientzertifikats auch ohne Zertifikat möglich sein sollte.

- Aktivieren Sie die Authentifizierungsmethode per 802.1x nachdem SCEP konfiguriert wurde.

  Der Client wird für die Zertifikatsanforderung eine Verbindung zum SCEP-Server ohne Authentifizierung versuchen und erst nach Erhalt des Zertifikats die Authentifizierung verwenden.

Bei WLAN-Verbindungen muss zunächst eine zertifkatslose PSK-Verschlüsselung eingerichtet werden, über diese Verbindung holt sich der Client dann das Zertifikat, anschließend kann die WLAN-Verbindung wieder umkonfiguriert werden.

Während die o.g. Methode für Ethernetanbindungen auch über UMS funktioniert, kann die Erstkonfiguration des WLANs nur direkt am Client erfolgen, da dieses standardmäßig deaktiviert ist.

8.6. Routing

Auf dieser Setupseite können Sie bei Bedarf zusätzliche Netzwerkstrecken angeben.

- Geben Sie im Feld **Interface** „eth0", „eth1" oder „wlan0" an, d.h. Interface 1+2 bzw. Wireless LAN.

Sie können insgesamt bis zu fünf zusätzliche Netzwerkstrecken angeben.

8.7. Hosts

Wenn kein DNS (Domain Name Service) verwendet wird, können Sie eine Liste mit Hosts angeben, um die Übersetzung zwischen Ihrer IP-Adresse, dem Full Qualified Host Name und dem Short Host Name zu ermöglichen.

Klicken Sie auf **Hinzufügen**, um das Dialogfenster zu öffnen.

1. Geben Sie die **IP-Adresse** des Hosts ein, den Sie hinzufügen möchten.
2. Geben Sie den **Full Qualified Host Name** an (z. B. <mailserver.igel.de>).
3. Geben Sie den **Short Host Name** des Hosts an (z. B. <mailserver>).
4. Bestätigen Sie die Eingabe mit **OK**.

   Der angegebene Host wird jetzt der Rechnerliste hinzugefügt.

8.8. Netzlaufwerke

Unter **Netzlaufwerke** bestimmen Sie sowohl die Laufwerke, die beim Start verbunden werden sollen, wie auch die zugehörigen Anmeldedaten.

Für jedes Laufwerk können Sie einen Laufwerksbuchstaben vergeben:

- Wird kein Buchstabe eingetragen, so muss das Laufwerk später manuell verbunden werden.
- Wenn im IGEL Setup die Anmeldedaten für den jeweiligen Server hinterlegt wurden, werden keine Anmeldedaten mehr angefordert.
- Sollte der vergebene Buchstabe bereits reserviert sein, so wird nur das zuerst verbundene Laufwerk angezeigt, für das zweite wird ein Fehlereintrag im Eventlog erstellt.



Figure 77: Netzlaufwerke hinzufügen

8.8.1. NFS

Mit NFS (Network File System) können Sie über das Netzwerk Dateien freigeben. Der NFS-Server exportiert eine Systemdatei, und der NFS-Client (Ihr Thin Client) verbindet diese Datei mit einem Einhängepunkt seines eigenen Dateisystems. Das exportierte Dateisystem wird dann ein logischer Bestandteil des Thin Client-Dateisystems, bleibt jedoch physisch auf dem Server.

> Um einen NFS-Mount einzurichten, muss der Server zunächst konfiguriert werden. Detaillierte Informationen zu NFS finden Sie auf den entsprechenden Handbuchseiten Ihres Serverbetriebssystems.

So geben Sie über den NFS-Server Dateien frei:

➢ Klicken Sie **Hinzufügen**, um das Dialogfenster für NFS zu öffnen.

Sie erhalten folgende Eingabemöglichkeiten:

Aktiviert	Der NFS-Mount ist standardmäßig aktiviert und wird bei jedem Systemstart eingehängt. Deaktivieren Sie den Eintrag, wenn das freigegebene Dateisystem nicht durchgängig benötigt wird.
Lokales Verzeichnis	Angabe des lokalen Verzeichnisses, in das die Freigabe im lokalen Dateisystem des Thin Clients eingehängt werden soll.
Server	Namen oder die IP-Adresse des NFS-Servers, der die Freigabe bereitstellt.
Pfadname	Angabe des Pfadnamens, wie er vom NFS-Server exportiert wurde.

8.8.2. Windows Laufwerk - SMB

SMB wird von Microsoft Windows für die Freigabe von Festplatten und Druckern verwendet. Da Unix (einschließlich Linux) dieses Protokoll mit den Tools der Samba-Suite ebenfalls verarbeiten kann, ist es möglich, Festplatten und Drucker gemeinsam mit Windows-Hosts zu nutzen. Deshalb können auf dem Thin Client SMB-Freigaben von Windows- oder Unix Samba-Hosts eingebunden werden.

> Das SMB-Protokoll wird nur für die Freigabe von Dateien über das Netzwerk genutzt (nicht für Drucker). Freigaben, die eingehängt werden sollen, müssen zunächst auf dem Windows- oder Unix-Host erstellt werden.

Lokales Verzeichnis	Angabe des lokalen Verzeichnisses, in das die Freigabe im lokalen Dateisystem des Thin Clients eingehängt werden soll.
Server	Für einen Windows-Host muss hier der Net BIOS-Name eingegeben werden. Bei einem Unix Samba-Host muss der Hostname oder die IP-Adresse verwendet werden.
Freigabename	Pfadname, wie er vom Windows- oder Unix Samba-Host exportiert wurde.
Benutzername/Passwort	Angabe von Benutzername und Passwort Ihres Benutzerkontos auf dem Windows- oder Unix Samba-Host
Aktiviert	Standardmäßig ist der SMB-Mount aktiviert und wird bei jedem Systemstart eingehängt.
Schreibbar für Benutzer	Wenn diese Option aktiv ist, kann der angemeldete Benutzer Daten schreiben. Dies ist sonst nur durch root möglich.

8.9. Systemweiter Proxy

Konfigurieren Sie, für welche Kommunikationsprotokolle ein systemweiter Proxy verwendet werden soll:

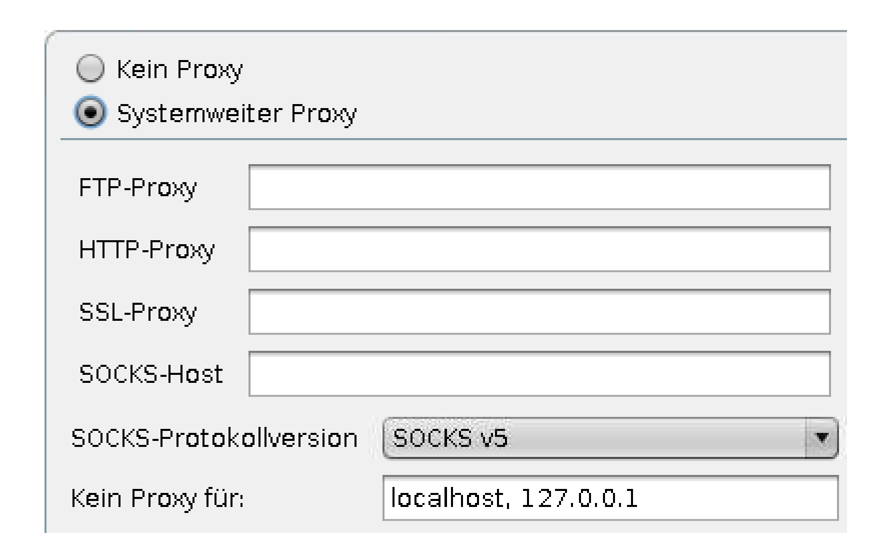


Figure 78: Systemweiter Proxy

9. Geräte

- Klicken Sie auf **Hardwareinformationen** (Seite 71), um einen Überblick über Ihren IGEL Thin-Client zu erhalten.

9.1. Drucker

Richten Sie hier einen Drucker für ICA-Sitzungen ein.

Mit der Funktion **Client Drucker aktivieren** wird der lokal angeschlossene Drucker des Thin Clients für Ihre ICA-Sitzungen verfügbar gemacht, vorausgesetzt, er wurde nicht serverseitig deaktiviert.

Die Drucker müssen auf der Seite **Geräte→Drucker→CUPS→Drucker** eingerichtet sein und dort für das Mapping in ICA-Sitzungen freigegeben werden, siehe *ICA-Sitzungen* (Seite 34).

Da der Thin Client die eingehenden Druckaufträge lediglich in eine Warteschlange stellt, müssen Sie den Drucker auf dem Server installieren. Gehen Sie dabei auf die übliche Weise vor: **Start→Einstellungen→Drucker** usw.

> Beachten Sie, dass Sie auf dem Terminal an das der Drucker angeschlossen ist, als Administrator angemeldet sein müssen.

9.1.1. CUPS - Common UNIX Printing System

Das Common UNIX Printing System™ (oder CUPS) ist die Software, mit der Sie aus Anwendungen heraus drucken können, wie z. B. aus diesem Webbrowser.

CUPS wandelt die von der Anwendung produzierten Seitenbeschreibungen, wie "Absatz einfügen", "Linie zeichnen" usw., in vom Drucker lesbare Daten um und sendet diese Informationen an den Drucker.

CUPS kann mit der entsprechenden Konfiguration Druckgeräte über die folgenden Anschlüsse verwenden:

- Parallel (LPT 1, LPT 2)
- Seriell (COM1, COM2, USB COM1, USB COM2 – mit USB-Seriell-Adapter)
- USB (1. und 2. USB-Drucker)
- Netzwerk (TCP/IP, LPD, IPP)

Drucker	Hier können Drucker erzeugt und bearbeitet werden. ➢ Definieren Sie im Bearbeitungsdialog einen Druckernamen, der mit einem Buchstaben beginnt.
Allgemein	➢ Wählen Sie unter **Drucker Anschluss** den Schnittstellentyp für lokal angeschlossene Drucker bzw. das Netzwerkprotokoll für Netzwerkdrucker. ➢ Geben Sie in Abhängigkeit davon die jeweiligen Konfigurationsdaten für die Schnittstelle bzw. den Netzwerkdrucker ein. ➢ Wählen Sie unter **Hersteller und Druckernamen** den lokalen Druckertreiber aus.
Mapping in Sitzungen	Drucker in NX-Sitzungen mappen: Macht den Drucker in NX-Sitzungen verfügbar. Drucker in ICA-Sitzungen mappen: Macht den Drucker in ICA-Sitzungen verfügbar. Drucker in RDP-Sitzungen mappen: Macht den Drucker in RDP-Sitzungen verfügbar.

Die restlichen Parameter dienen der Auswahl des Druckertreibers in ICA- und RDP-Sitzungen auf Windows-Serverseiten.

- Geben Sie den Namen des Treibers unter Windows an, der verwendet werden soll.

  Falls er nicht in der Liste aufgeführt ist, kann er unter **Benutzerdefinierten Windows Treibernamen verwenden** angegeben werden.

Im Normalfall werden die Druckdaten beim Druck in ICA- und RDP-Sitzungen vom Windows-Druckertreiber für das Druckermodell aufbereitet und vom Thin Client unverändert zum Drucker durchgeleitet. Eine Ausnahme ist in ICA-Sitzungen die Verwendung des Windows-Treibers:

Hersteller: Generic,
Modell: Generic PostScript
(Citrix Universal Printer Driver Postscript)

In diesem Fall werden die Druckdaten auf dem Thin Client mit Hilfe des oben unter **Drucker** definierten Druckertreibers für das Druckermodell aufbereitet. Dies benötigt je nach Größe des Druckauftrags Ressourcen auf dem Thin Client.

IPP Printer Sharing (IPP-Druckerfreigabe)	Das IPP (Internet Printing Protocol) bietet folgende Konfigurationsoptionen:	
	Netzwerk oder Host für die Freigabe lokaler Drucker	Ermöglicht das Drucken auf dem lokalen Gerät entweder aus dem lokalen oder globalen Netzwerk.
	Enable IPP Printer Browsing (IPP Drucker Browsing)	Führen Sie eine Suche nach freigegebenen Druckern im lokalen oder globalen Netzwerk durch, und zeigen Sie Ihre freigegebenen Drucker im Netzwerk an. Ein freigegebener Drucker ist im Netzwerk sichtbar, aber das Drucken aus dem Netzwerk ist bei fehlender Autorisierung eventuell nicht möglich.

9.1.2. LPD - Line Printer Daemon

LPD-Drucker werden vom BSD-Drucksystem verwendet und werden auch von Windows-Servern unterstützt.

LPD-Druckserver aktivieren	Macht den Thin Client zum LPD-Druckserver. Die unter 11.2.1.1 definierten CUPS-Drucker können unter ihrem Druckernamen als Warteschlangenname über das LPD-Protokoll angesprochen werden.
Druckdatenumwandlung	Versucht automatisch zu erkennen, ob die Druckdaten über den lokalen Druckertreiber aufbereitet werden müssen oder nicht. Die Option **keine** leitet die Druckdaten immer unverändert an den Drucker weiter.
Max. gleichzeitige Verbindungen	Begrenzt die Anzahl gleichzeitig angenommener Druckaufträge.
LPD-Zugang einschränken	Legt fest, aus welchen Subnetzen bzw. von welchen Hosts Druckaufträge angenommen werden.

9.1.3. TCP/IP

Sie können an Ihr Gerät angeschlossene Drucker einem TCP/IP-Port zuweisen. Aktiviert ist standardmäßig der Anschluss LPT1 (TCP/IP-Port 3003). Der Drucker kann an einen der folgenden Anschlüsse angeschlossen werden, sofern sie am Gerät verfügbar sind:

- Serieller Anschluss (COM 1 oder COM 2)
- Paralleler Anschluss (LPT 1)
- USB (USBLP 1)
- Zusätzliche serielle Anschlüsse: USB-Adapter oder Erweiterungskarte von Perle

An seriellen Schnittstellen erfolgt die Weiterleitung der Daten bidirektional, so dass auch andere serielle Geräte wie z. B. Barcodescanner oder Waagen betrieben werden können.

9.1.4. ThinPrint

ThinPrint ermöglicht die ressourcenorientierte Reduzierung der Bandbreite, die für Druckauftragsübertragungen bereitgestellt wird. Der **ThinPrint**-Client druckt entweder direkt an Druckern, die an einer lokalen Schnittstelle (seriell, parallel oder USB) angeschlossen sind, an einen LPD-Netzwerkdrucker oder an einen auf dem Thin Client definierten CUPS-Drucker.

Auf der **ThinPrint**-Setupseite finden Sie folgende Parameter:

Portnummer	Geben Sie die Portnummer ein, über die der ThinPrint-Dämon kommunizieren soll. Vergewissern Sie sich, dass die Portnummer auf dem ThinPrint-Client und dem ThinPrint-Server dieselbe ist (die Kommunikation ist ansonsten nicht möglich).
Bandbreite	Geben Sie einen Bandbreitenwert (in Bit pro Sekunde) ein, der kleiner oder gleich dem auf dem ThinPrint-Server festgelegten Wert ist. Ein größerer Wert, die Deaktivierung der Clientkontrolle oder gar keine Eingabe bedeutet, dass die ThinPrint-Serverwerte angewendet werden.
Wartezeit zwischen Druckversuchen	Maximale Wartezeit bei blockiertem Drucker (in Sekunden)
Anzahl der Druckversuche	Anzahl der Versuche, einen Drucker zu kontaktieren, um einen Druckauftrag zu starten.

Auf der Seite **Drucker** wird die Liste der **ThinPrint**-Drucker angezeigt.

➢ Verwalten Sie hier Druckerkonfigurationen, indem Sie sie hinzufügen, bearbeiten oder löschen.

Die Seite gibt Ihnen einen Überblick über die vorkonfigurierten **ThinPrint**-Drucker:

Aktiv	Gibt an, ob der Drucker sichtbar ist oder nicht.
Name des Druckers	Name, unter dem der Drucker angesprochen werden kann.
Druckerklasse	Name der Druckerklasse - optional, max.7 Zeichen, ohne Leerzeichen
Gerät	Hier gibt es folgende Möglichkeiten: • + /dev/ttyS0, /dev/ttyS1, ... serielle Schnittstelle • + /dev/lp0, /dev/lp1, ... parallele Schnittstelle • + /dev/usblp0, /dev/usblp1, ... USB-Drucker • + Name eines CUPS-Druckers mit Druckeranschluss LPD-Netzwerkdrucker: ThinPrint-Client druckt direkt über das Netzwerk zum LPD-Netzwerkdrucker. • + Name eines sonstigen CUPS-Druckers: ThinPrint-Client leitet Druckaufträge an entsprechenden Drucker im CUPS-Drucksystem weiter.
Standard	Legt das ausgewählte Gerät als Standarddrucker fest.

9.2. Speichergeräte

Konfigurieren Sie hier Ihre USB-Speichergeräte.

9.2.1. USB-Speicher-Hotplug

In diesem Bereich geben Sie an, wie USB-Geräte eingerichtet werden.

Die wichtigsten Angaben sind

- Dynamic Client Drive Mapping aktivieren. Für ICA-Sitzungen werden dann USB-Massenspeichergeräte dynamisch in der Sitzung hinzugefügt und wieder entfernt.
  Damit sind die folgenden Einstellungen nur noch für Sitzungen ohne Dynamic Client Drive Mapping gültig:
- die Anzahl der möglichen Geräte,
- die Zuweisung von Laufwerksbuchstaben,
- die für die Benutzer in ICA-Sitzungen zur Verfügung stehende Zugriffsart (Lese- und/oder Schreibzugriff).

☐ Dynamic Client Drive Mapping aktivieren

Zahl der USB-Speicher-Hotplug-Geräte: 0
☐ Eigener Laufwerksbuchstabe für USB-Speicherlaufwerke.
USB-Speicherlaufwerke mit diesem Laufwerksbuchstaben starten: A
ICA-Lesezugriff auf USB-Speicher-Hotpluggeräte: Ja
ICA-Schreibzugriff auf USB-Speicher-Hotpluggeräte: Ja

☑ Signalton des USB-Speicher-Hotplug verwenden
☑ Meldungen des USB-Speicher-Hotplug anzeigen
Meldungen nach dieser Zeit ausblenden: 0
☑ Gerätebeschreibung anzeigen
☑ Fehler anzeigen
☑ Lokales Verzeichnis anzeigen
☑ Serverlaufwerk anzeigen

Figure 79: USB-Speicher-Hotplug

Bei aktiviertem Dynamic Client Drive Mapping werden neu angeschlossene Geräte automatisch erkannt. Der Thin Client gibt ein akustisches Signal aus, und es öffnet sich ein Pop-up-Fenster, in dem darüber informiert wird, dass ein neues Gerät benutzbar ist.

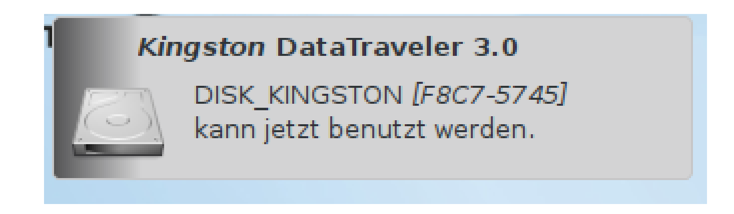


Figure 80: Gerät kann benutzt werden

> Hinweis: Bevor Sie das Speichergerät vom Thin Client trennen, müssen Sie es sicher entfernen. Ansonsten droht Datenverlust auf dem Speichergerät!

Zum sicheren Entfernen benutzen Sie die *Laufwerksverwaltung* (Seite 72) oder das Auswerfen-Symbol in der Taskleiste:



Figure 81: Sicher entfernen

In Vollbildsitzungen können Sie Geräte sicher entfernen, indem Sie die *Laufwerksverwaltung* (Seite 72) per Hotkey aufrufen. Alternativ können Sie die *Allgemeine Werkzeugleiste* (Seite 82) verwenden.

Erhalten Sie die Warnung **Das Geräte wird noch benutzt!** darf dieses nicht entfernt werden, da sonst Datenverlust droht.

- Beenden Sie zuerst entweder das genannte Programm oder schließen Sie alle geöffneten Dateien oder Verzeichnisse innerhalb einer Sitzung, die sich auf dem genannten Geräte befinden.
- Versuchen Sie danach erneut, das Geräte wie oben beschrieben sicher zu entfernen.

> Es kann notwendig sein, einige Sekunden zu warten, bevor alle Dateien innerhalb einer Sitzung tatsächlich geschlossen wurden. Wiederholen Sie das sichere Entfernen so lange, bis keine Fehlermeldung mehr angezeigt wird.

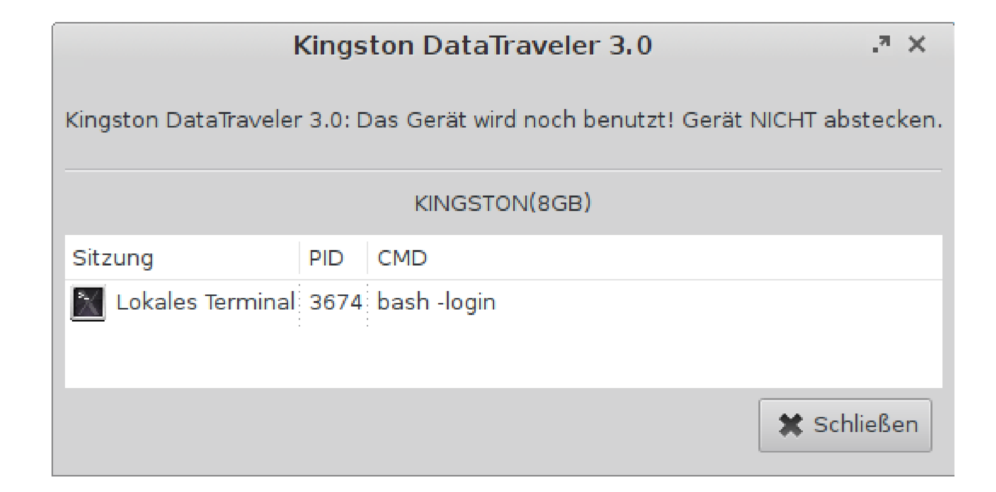


Figure 82: Das Gerät wird noch benutzt.

9.2.2. Automount-Geräte

Definieren Sie hier die Geräte, die automatisch beim Zugriff eingehängt werden sollen:

Liste der Automount-Geräte	Überblick über die Automount-Geräte - Die am häufigsten verwendeten Geräte, wie das Diskettenlaufwerk, CD-ROM usw., sind vorkonfiguriert.
Bearbeiten	Öffnen und Aktivieren eines der vordefinierten Geräte
Hinzufügen	Manuelle Konfiguration von Geräten, die nicht in der Automount-Geräteliste vordefiniert sind.
Name	Vergabe eines Gerätenamens - Dieser Name wird als Unterverzeichnisname übernommen, das in `/autofs/` erstellt wird.
Gerät	Auswahl eines geeigneten Gerätesynonyms - Auch eine manuelle Eingabe ist möglich.
Dateisystemtyp	Definition des Dateisystems - Üblicherweise sollte die Option **auto** verwendet werden. Wenn Sie jedoch **ext2** verwenden oder ein Problem auftritt, geben Sie das von Ihnen genutzte Dateisystem eindeutig an.
Automount Time-out	Regelung der Time-out-Zeitspanne - Geben Sie in Sekunden an, wie lange das System nach einem Zugriff auf Ihre Geräte warten soll, bevor sie ausgehängt werden. Die Zeitspanne reicht von 0 bis 600 Sekunden (100 Minuten).

> Setzen Sie die Time-out-Dauer nicht auf Null! Das kann zu Datenverlusten führen.

9.3. USB-Zugriffskontrolle

USB-Geräte können anhand von Regeln für die Verwendung am Thin Client zugelassen oder verboten werden, dabei sind auch Unterregeln für Geräte oder Geräteklassen möglich.

1. Aktivieren Sie die USB-Zugriffskontrolle unter **Geräte→USB-Zugriffskontrolle**.
2. Wählen Sie eine **Vorgaberegel** (Default Verhalten), welche die Verwendung von USB-Geräten grundsätzlich erlaubt oder verbietet.
3. Erweitern Sie die allgemeine Vorgabe um Klassenregeln und Geräteregeln, in denen Sie festlegen, wie mit bestimmten Klassen oder Geräten verfahren werden soll.

   > Geräteklassen können z.B. Eingabegeräte, Drucker oder Massenspeicher sein, Geräteregeln beziehen sich auf den Hersteller, das Produkt oder das konkrete Gerät (identifiziert über dessen Universally Unique Identifier UUID).

Beispiel:

- Die Vorgaberegel verbietet die Verwendung von USB-Geräten am Thin Client.
- Alle Eingabegeräte (Human Interface Devices HID) sind jedoch für die Verwendung zugelassen.
- Außerdem ist das USB-Speichergerät mit der UUID 67FC-FDC6 ebenfalls zulässig.

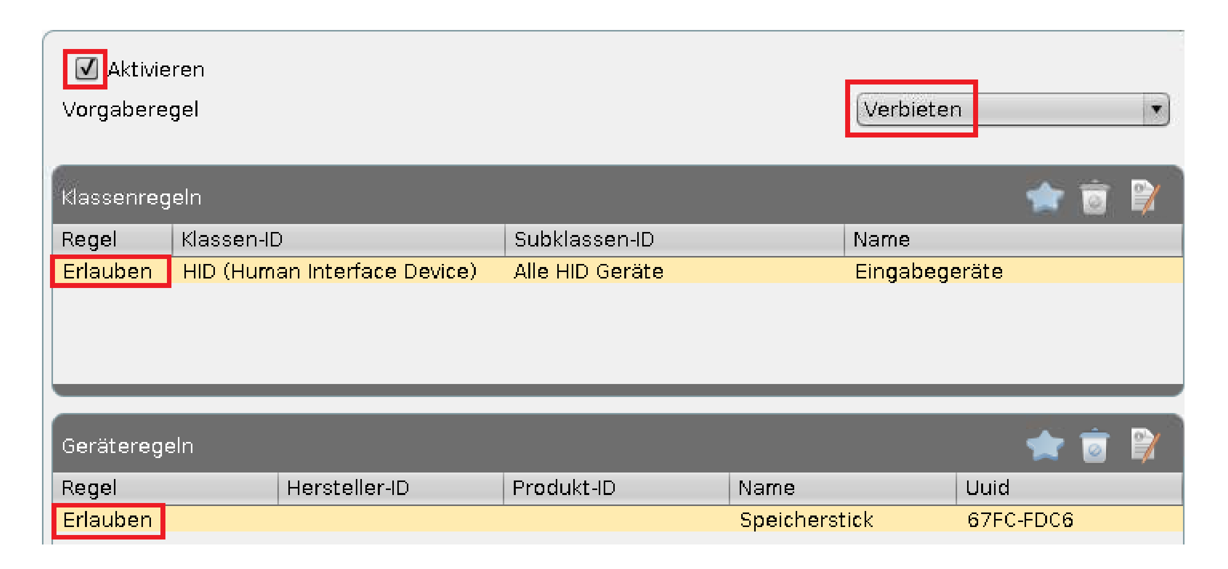


Figure 83: USB-Zugriffskontrolle

Andere USB-Speicher, -Drucker oder sonstige USB-Geräte können mit dieser Einstellung nicht am Thin Client verwendet werden.

9.4. PC/SC-Schnittstelle

PC/SC ist ein Dienst, der Anwendungsprogrammen Smartcardleser und eingesteckte Smartcards zur Verfügung stellt. RDP- und ICA-Verbindungen erlauben es, die clientseitigen Smartcardleser und Smartcards serverseitigen Applikationen bereitzustellen. Außerdem können lokale Applikationen, wie z. B. Browser, Smartcards in den Lesern nutzen. Für diese Funktionalitäten muss der PC/SC-Dämon aktiviert sein.

➢ Klicken Sie **PC/SC Dämon aktivieren**, um die PC/SC-Schnittstelle auf dem Thin Client zu nutzen.

Im Fenster **Momentan aktive PC/SC-Geräte** sehen Sie die aktuell zur Verfügung stehenden Smartcardleser. Unterstützt sind optionale interne Leser und eine Reihe von USB-Smartcardlesern. Die komplette Liste der unterstützten Geräte finden Sie in der IGEL Hardware Datenbank.

10. Sicherheit

Um unbefugte Zugriffe im Thin Client-Setup zu vermeiden, die ein tieferes Vordringen in Ihr Netzwerk ermöglichen könnten, sollte nach der Anfangskonfiguration unbedingt ein Administratorpasswort eingerichtet werden.

➢ Verwenden Sie ein zusätzliches Benutzerpasswort, das sehr variable Optionen bietet, um eingeschränkte Konfigurationen durch den Benutzer zuzulassen.

10.1. Passwort

➢ Richten Sie unter **Passwort** ein Administratorpasswort sowie ein Benutzerpasswort ein.

Administrator- und Benutzerpasswort	Vergeben von Passwörtern für das Administrator- bzw. Benutzerkonto. Das Setup wird in dem Fall durch das Administratorkennwort geschützt, es sei denn, es wurden Bereiche auch für den Benutzer freigegeben.

Durch die Aktivierung dieses Passworts wird das IGEL Setup, der Shell-Zugriff in Xterm und der Zugriff auf die Konsole auf den Administrator eingeschränkt. Die Nutzung der Option **Reset to factory defaults - Z**urücksetzen auf Werkseinstellungen - ist nur mit diesem Passwort möglich. Wird das Setup durch ein Administratorpasswort gesperrt, lassen sich für den Benutzer einzelne Setupseiten freischalten. Siehe *Setupseiten für Benutzer freigeben* (Seite 19).

Setupbenutzer	Erlaubt dem Benutzer den Zugriff auf das lokale Setup.
Benutzerkonto für Fernzugriff	Legt ein Passwort für den Remote-Sitzungsnutzer (SSH) fest.

Achten Sie darauf, dass das richtige Tastaturlayout aktiviert ist, wenn Sie ein Passwort eingeben. Denn Sie sehen statt der Zeichen nur Sternchen und können dann nicht nachvollziehen, warum das Passwort nicht akzeptiert wurde.

10.2. Anmeldung

➢ Konfigurieren Sie hier eine lokale Anmeldung am Thin Client. Dies kann entweder über die IGEL Smartcard erfolgen oder über das Kerberos-Protokoll z. B. in einer Windows-Domäne.

10.2.1. IGEL Smartcard

Anmeldung mit IGEL Smartcard	Aktivieren der lokalen Anmeldung am Thin Client mit IGEL Smartcard. Auf der Smartcard abgelegte Sitzungen werden verfügbar. Ohne Smartcard und optionales Passwort ist der Thin Client gesperrt.
IGEL Smartcard ohne Sperren des Desktops aktivieren	Aktivieren von auf der Smartcard abgelegten Sitzungen nach Eingabe eines optionalen Passworts. Der Thin Client wird auch ohne Smartcard nicht gesperrt.
Firmenschlüssel	Gemeinsamer Schlüssel der Smartcards und Thin Clients. Zur Smartcard-Personalisierung siehe *IGEL Smartcard* (Seite 115).

Sie können die optionale IGEL Smartcard für die lokale Authentifizierung und die personalisierte Sitzungskonfiguration („Flying Doctor-Szenario") verwenden.



Figure 84: IGEL-Smartcard

So verwenden Sie die IGEL Smartcard mit dem internen Kartenleser oder einem externen Lesegerät (USB):

1. Aktivieren Sie die IGEL Smartcardlösung unter **Sicherheit→ Anmeldung→Smartcard** in der Setupanwendung.
2. Geben Sie einen **Firmenschlüssel** zum Beschreiben Ihrer IGEL Smartcard ein.
3. Speichern Sie die Einstellung, bevor Sie mit der Personalisierung der Karte beginnen.
4. Im Fenster **Personalisierung** können Sie ein Anmeldepasswort festlegen und Sitzungen zur Karte hinzufügen.

Sitzungskonfigurationen werden auf dem IC (integrierter Schaltkreis) der Karte gespeichert, und die Sitzung kann auf jedem beliebigen IGEL Thin Client verwendet werden, der die Karte liest.

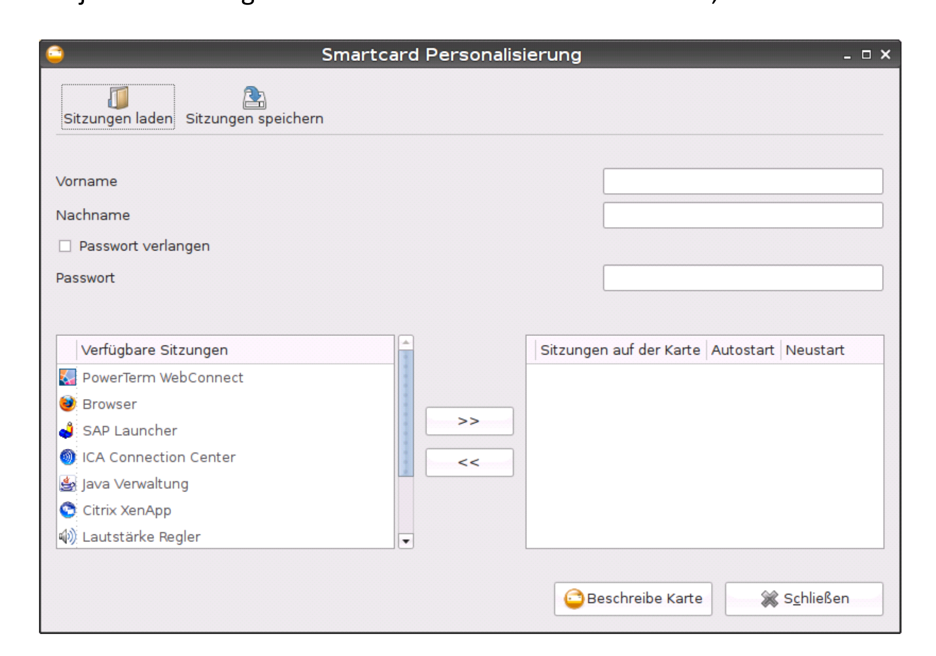


Figure 85: Smartcardpersonalisierung

Firmenschlüssel

Die IGEL Smartcardlösung beinhaltet auch einen **Firmenschlüssel**. Es handelt sich dabei um einen zusätzlichen Code, der auf die Smartcard geschrieben wird und mit dem Code des verwendeten Terminals übereinstimmen muss. Wenn die beiden Codes nicht übereinstimmen, kann die Smartcard auf diesem Terminal nicht verwendet werden. Dies ist eine zusätzliche Sicherheitsmaßnahme, um sicherzustellen, dass nicht von außerhalb Ihres Unternehmens auf Ihre Terminals zugegriffen werden kann. Auch im Unternehmen kann sie verwendet werden, um den Zugriff von Mitarbeitern auf bestimmte Terminals zu begrenzen.

Benutzer und Passwort speichern

So speichern Sie Benutzer und Passwort für die Authentifizierung:

➢ Geben Sie den Vor- und Nachnamen des Benutzers ein (auf jeweils 12 Zeichen begrenzt).

Sie werden dann mit diesem Namen zur Eingabe des Passworts aufgefordert.

> Wenn die Option **Passwort verlangen** aktiviert wurde, wird immer beim Einlegen einer Smartcard ein Pop-up-Fenster geöffnet. Bei falscher PIN-Eingabe wird der Zugriff auf das Terminal verweigert.

Gehen Sie folgendermaßen vor, wenn die Smartcard lediglich verwendet wird, um den Zugriff auf das Terminal zu kontrollieren:

1. Legen Sie eine passende Smartcard ein.
2. Klicken Sie **Beschreibe Karte**, um die Daten auf die Karte zu schreiben.
3. Entfernen Sie die Smartcard, wenn der Schreibvorgang erfolgreich abgeschlossen ist.

Nun können Sie die nächste Smartcard programmieren.

Sitzungen speichern

Sitzungen auf der Smartcard speichern

Wenn ein Mitarbeiter mehrere unterschiedliche Terminals nutzt oder die Terminals von vielen verschiedenen Mitarbeitern verwendet werden, kann es sinnvoll sein, die vom Mitarbeiter genutzten Sitzungen auf seiner Smartcard statt auf dem Terminal zu speichern. Auf diese Art und Weise muss der Benutzer lediglich die Anwendungen aufrufen können, die er für die Ausführung seiner Aufgaben benötigt.

So speichern Sie Sitzungen auf der Smartcard:

1. Legen Sie die Smartcard des Mitarbeiters in das Terminal ein.

   Die von ihm genutzten Anwendungen werden auf dem Terminal angezeigt.

2. Erstellen Sie die Sitzungen, die Sie der Smartcard auf dem Terminal hinzufügen möchten, einschließlich einer Autostartoption und einer Personalisierung der Anmeldeinformationen.

   > Sie können neben dem Vor- und Nachnamen des Kartenbenutzers und eines optionalen Passworts auch die Sitzungen zur Smartcard hinzufügen, die im Bereich **Verfügbare Sitzungen** angezeigt werden. Stellen Sie vor dem Beschreiben der Karte sicher, dass die hinzugefügten Sitzungen auch eine Startoption besitzen, also z.B. auf dem Desktop oder im Starter für Sitzungen angezeigt werden.

3. Klicken Sie auf **Beschreibe Karte**, um die Daten auf der Smartcard zu speichern, nachdem Sie alle gewünschte Sitzungen hinzugefügt haben.

Karte testen

- Testen Sie die erstellte Karte.

Nach dem Warmstart und dem Einlegen der Smartcard werden die Sitzungen sofort auf der Arbeitsfläche angezeigt. Es wird jede Sitzung ausgeführt, für die Sie das automatische Starten bei Einlegen der Smartcard festgelegt haben.

10.2.2. AD/Kerberos

Anmelden mit Kerberos	Aktivieren der lokale Anmeldung am Thin Client über das Kerberos-Protokoll. Hierfür muss auch *AD/Kerberos konfiguriert* (Seite 118) sein. Die Anmeldung kann in einigen Sitzungsarten (ICA, RDP) für Single Sign-on genutzt werden.
Verknüpfung zum Abmelden	Konfigurieren, auf welche Weise(n) sich der Benutzer abmelden kann.

10.2.3. Auto Logoff

Definieren Sie eine **Auto Logoff** Aktion, welche bei der Beendigung der letzten Instanz eines Sitzungstyps ausgeführt wird:

1. Rufen Sie die Setup Seite **Sicherheit→Anmeldung→Auto Logoff** auf.
2. Wählen Sie einen **Sitzungstyp**.

3. Wählen Sie einen **Befehl (Auto Logoff Command)**.
4. Speichern Sie die Einstellung mit **Übernehmen** oder **OK**.

Wird die letzte Sitzungsinstanz des gewählten Typs geschlossen, so führt das System die eingestellte Aktion aus.

Der Befehl **Shutdown** führt die eingestellte Vorgabeaktion aus, prüfen Sie diese unter **System→Energie→Herunterfahren**.

Der Befehl **Logoff** ist wirkungslos, solange Sie nicht eine Anmeldemethode definiert haben unter **Sicherheit→Logon** (Smartcard, Active Directory/Kerberos oder IGEL Shared Workplace). Der **Logoff** Befehl kann nicht zusammen mit einer Appliance verwendet werden - in diesem Fall arbeiten nur die Befehle **Shutdown/Suspend** und **Reboot** korrekt.

Wenn Sie Auto Logoff Befehle in einer Appliance einsetzen, stellen Sie sicher, dass der passende Sitzungstyp gewählt wurde - z.B. Horizon bei Einsatz der VMware Horizon Appliance.

10.3. AD/Kerberos-Konfiguration

➢ Aktivieren und konfigurieren Sie Kerberos auf diesen Setupseiten, um diesen Dienst für die Anmeldung und Single Sign-on zu nutzen.

Standarddomäne	Angeben des Standard-Kerberos-Bereichs für den Client. Legen Sie diesen Wert so fest, dass er Ihrem Kerberos-Bereich (Windows-Domäne) entspricht.
DNS-Suche nach Domänencontrollern	Festlegen, ob DNS SRV Records benutzt werden sollen, um die Key Distribution Centers (KDCs, Schlüsselverteilungscenter, Domänencontroller) und andere Server für einen Realm (Bereich) zu finden, falls sie nicht angegeben sind.
DNS-Suche nach Domäne	Festlegen, ob DNS TXT Records benutzt werden sollen, um den Kerberos-Realm eines Hosts zu bestimmen.
Adresslose Tickets anfordern	Falls gesetzt, ist das erste Kerberos-Ticket adresslos. Dies kann erforderlich sein, wenn der Client sich hinter einem NAT- Gerät (Network Address Translation) befindet.

10.3.1. Realm 1-4

Hier können bis zu 4 Realms konfiguriert werden, an denen eine Anmeldung ermöglicht wird.

Realm	Der Name des Realms/der Domäne, an dem/der Sie sich authentifizieren möchten.
KDC-Liste	IP- oder FQDN-Liste des Key Distribution Center (Domänencontroller) für diesen Realm. Eine optionale Portnummer, mit vorangestelltem Doppelpunkt, kann an den Hostnamen angehängt werden.

10.3.2. Domain-Realm-Zuordnung

Die **Domain-Realm-Zuordnung** bietet eine Übersetzung eines Hostnamens in den Kerberos-Realm-Namen für die Services, die von diesem Host bereitgestellt werden.

Standard Domain-Realm-Zuordnung	Sollte aktiv sein, falls DNS- und Realm-Namen übereinstimmen. Ansonsten müssen benutzerspezifische Einträge in der Liste erzeugt werden.
DNS-Host oder Domainname	Der Eintrag kann ein Hostname oder ein Domänenname sein. Domänennamen werden durch einen vorangestellten Punkt gekennzeichnet. Hostnamen und Domänennamen sollten in Kleinbuchstaben eingegeben werden.
Realm	Kerberos-Realm-Name für diesen Host oder diese Domäne

11. Systemeinstellungen

Wie bereits unter *Schnellinstallation* (Seite 6) erläutert, können in der Unterstruktur einige grundlegende Systemeinstellungen vorgenommen werden.

Datum und Zeit (Seite 120)

Update (Seite 121)

Fernadministration (Seite 122)

Spiegeln (Seite 123)

Fernzugriff (Seite 128)

Energie (Seite 128)

Firmwareanpassungen (Seite 136)

Registry (Seite 138)

11.1. Datum und Zeit

1. Klicken Sie auf **Datum und Zeit**, um diese Dialogseite zu öffnen.

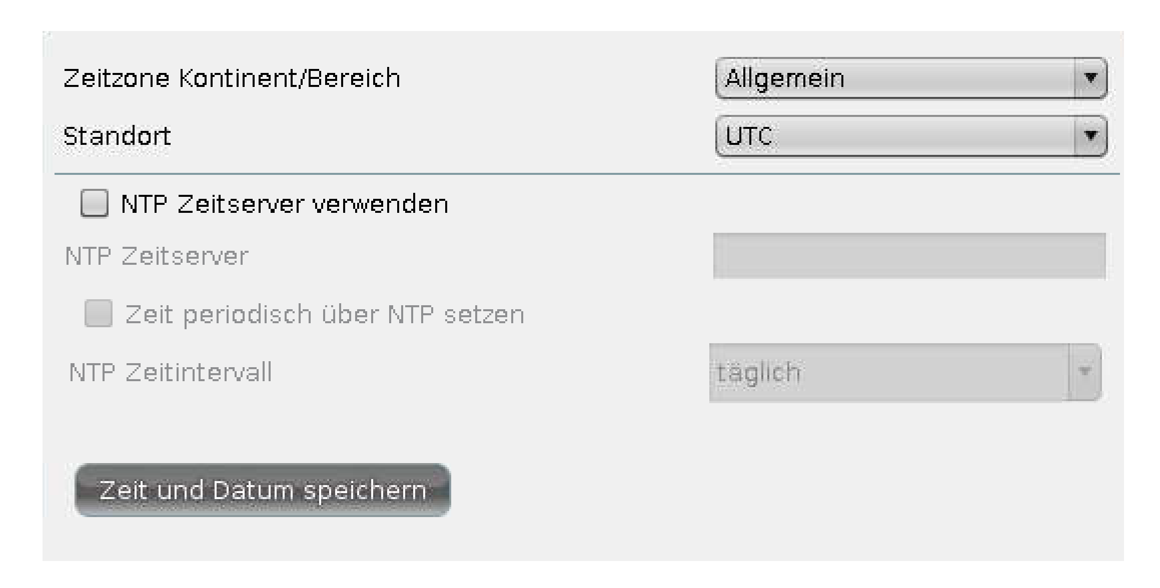


Figure 86: Zeit und Datum setzen

2. Nehmen Sie die gewünschten Änderungen vor.
3. Klicken Sie **Zeit und Datum speichern** um die Änderungen zu bestätigen.

> Wenn in Ihrem Netzwerk ein Zeitserver verfügbar ist, können Sie auch das Network Time Protocol (NTP) nutzen, um die aktuelle Uhrzeit und das aktuelle Datum automatisch während des Systemstarts und in definierten Intervallen abzurufen.

Achten Sie darauf, dass die Zeitzone korrekt gesetzt ist. Wählen Sie dazu über die Drop-down-Boxen die entsprechende Region aus.

> Beachten Sie, dass die GMT-Zeitzonen unter Linux üblicherweise im POSIX-Format vorliegen. Dies bedeutet, Sie müssen die tatsächliche Zeitdifferenz invertieren (z.B. wählen Sie für New York die Zone GMT+5 für "5 Stunden westlich von Greenwich", obwohl die Zeit in New York tatsächlich 5 Stunden hinter GMT liegt). Daher ist die Definition der Zeitzone über die Wahl von **Kontinent** und **Standort** zu bevorzugen.

Zusätzliche Informationen zur Aktualisierung von Zeitzoneninformationen (etwa bei Sommerzeitregelungen) finden Sie im FAQ Updating Timezone Information (Daylight Saving Time, DST)

11.2. Update - Firmwareupdate

Auf der Seite **Update** wird ein einfacher Dialog für die Aktualisierung Ihrer Thin Client-Firmware angezeigt. So läuft das normale Verfahren für die Aktualisierung Ihres Thin Clients ab:

1. Laden Sie sich das gewünschte Firmwareimage über die Seite www.myigel.biz vom IGEL Server herunter.
2. Entpacken Sie die ZIP-Datei (übliche Bereitstellungsform für Updates).
3. Speichern Sie alle Dateien im dafür vorgesehenen Verzeichnis auf Ihrem lokalen FTP- oder HTTP-Server oder in einem vom Client aus zugänglichen Laufwerk (z. B. USB-Stick, NFS-Freigabe etc.).
4. Nehmen Sie die erforderlichen Einstellungen (siehe unten) vor.
5. Speichern Sie die Änderungen und klicken Sie **Firmware aktualisieren**.

   Der Updateprozess wird nun automatisch fortgesetzt.

> Das Updateverfahren kann nicht über PPP/ISDN-Verbindungen durchgeführt werden. Verwenden Sie in diesem Fall ein lokales Speichermedium (USB-Stick) für die Bereitstellung des Updates.

Die folgenden Informationen müssen angegeben werden, um das Update zu starten (je nach gewähltem Protokoll variieren die notwendigen Angaben):

Protokoll	Auswählen des zu verwendenden Protokolls aus der Drop-down-Liste (FTP, HTTP, HTTPS usw.).
Servername und Port	Angabe des Namens oder der IP-Adresse des verwendeten Servers sowie des zu verwendenden Ports
Pfadname auf dem Server	Angabe des Verzeichnisses, in dem Sie die Updatedateien gespeichert haben - ausgehend vom Root-Verzeichnis
Benutzername	Angabe des Benutzerkontonamens
Passwort	Angabe des Passworts für diesen Benutzer/dieses Konto
Automatische Updatesuche	Neue Updates werden bei jedem Systemstart in der definierten Quelle gesucht und ggf. automatisch installiert.
Automatische Buddy-Server-Erkennung	Im Updateprozess nach Buddy-Update-Server im Netzwerk suchen und das Update von dort laden.

Best-Practice-Dokumente zum IGEL Linux Firmwareupdate finden Sie in der IGEL Knowledge Base (http://edocs.igel.com). Auch die *Support-FAQ* (*http://faq.igel.com*) enthalten Artikel zur Aktualisierung der Firmware.

11.2.1. Buddy Update

Unter **Buddy Update** können Sie Ihren Thin Client als **Updateserver** für andere IGEL Thin Clients festlegen. Wenn Sie einen Thin Client als Updateserver nutzen, kann nur das FTP-Protokoll für die Aktualisierung der Firmware verwendet werden. Es können mehrere Thin Clients als **Buddy Update**-Server im Netzwerk eingerichtet werden.

Thin Clients ohne eingetragenen Updateserver suchen beim Update nach verfügbaren Servern, der erste erreichte Updateserver liefert das Update.

> Für weitere Informstionen lesen Siedas Best Practice Buddy Update in unserer Wissensdatenbank **eDocs**.

11.3. Fernadministration

Wenn der Thin Client durch einen IGEL UMS Server registriert wurde, wird unter **Fernadministration** die Serveradresse angezeigt.

Diese Registrierung können Sie auch vom Thin Client aus vornehmen:

1. Öffnen Sie den **Starter für Sitzungen**.
2. Starten Sie im Bereich **System** die Anwendung **UMS Registrierung**.
3. Tragen Sie **Adresse** und **Zugangsdaten** Ihres UMS Servers ein.

> Wenn ein entsprechender DNS-Eintrag für den UMS Server besteht, können Sie den Vorgabewert `igelrmserver` im Adressfeld belassen.

4. Optional: Wählen Sie ein **Zielverzeichnis** auf dem Server aus.

5. Optional: Definieren Sie ein **Strukturtag**, um den Thin Client entsprechend der UMS Verzeichnisregeln zu registrieren.

   > Strukturtags lassen sich auch über die DHCP-Option 226 an Thin Clients verteilen, um die automatische Registrierung und Sortierung in der UMS Datenbank zu unterstützen. Ein über DHCP erhaltenes Strukturtag hat bei der Registrierung an der UMS Vorrang gegenüber dem manuell eingetragenen Tag.

6. Klicken Sie **Registrieren**.

11.4. Spiegeln

Für Helpdesk-Zwecke können Sie den Client über die IGEL UMS oder über einen anderen VNC-Client (z. B. TightVNC) per Spiegelung beobachten. Die Optionen für die VNC-Funktionen sind:

Benutzer um Erlaubnis fragen	In einigen Ländern ist das unangekündigte Beobachten durch eine Spiegelung gesetzlich verboten. Deaktivieren Sie diese Option nicht, wenn Sie sich in einem dieser Länder befinden!
Eingaben vom entfernten Rechner aus zulassen	Wenn diese Option aktiviert ist, darf der Remote-Benutzer Tastatur- und Mauseingaben vornehmen, als wäre er der lokale Benutzer.
Passwort verwenden	Aktivieren Sie diese Option, um ein Passwort einzurichten, das der Remote-Benutzer eingeben muss, bevor er mit dem Spiegeln beginnen kann.
Bildfenster skalieren (Linux)	Der Bildschirminhalt des gespiegelten Thin Clients wird um einen Faktor verkleinert oder vergrößert übertragen.
Sicheres Spiegeln	Die Kommunikation wird per SSL/TLS gesichert und das Spiegeln ist nur als UMS-Administrator möglich.

> Weitere Parameter des VNC-Servers auf dem Thin Client sind in der IGEL Registry zugänglich (**Setup > System > Registry > network.vncserver**).

11.5. Sicheres Spiegeln (VNC mit SSL/TLS)

Die Funktion **Sicheres Spiegeln** erhöht die Sicherheit bei der Fernwartung eines Thin Clients über VNC an mehreren Stellen:

- Verschlüsselung: Die Verbindung zwischen dem spiegelnden Rechner und dem gespiegelten Thin Client wird verschlüsselt.

  Dies ist unabhängig vom verwendeten VNC-Viewer.

- Integrität: Nur Thin Clients in der UMS-Datenbank können gespiegelt werden.
- Autorisierung: Nur autorisierte Personen (UMS-Administratoren mit ausreichender Berechtigung) können Thin Clients spiegeln.

  Ein direktes Spiegeln ohne Anmeldung an der UMS ist nicht möglich.

- Limitierung: Nur das in der UMS konfigurierte VNC-Viewer-Programm (interner oder externer VNC-Viewer) kann zum Spiegeln verwendet werden.

  Das direkte Spiegeln eines Thin Clients durch einen anderen Thin Client wird ebenfalls unterbunden.
- Protokollierung: Verbindungen, die über das sichere Spiegeln aufgebaut werden, werden am UMS-Server im Log erfasst.

  Zusätzlich zu den Verbindungsdaten lassen sich auch die zugehörigen Benutzerdaten (spiegelnder UMS-Administrator, optional) im Log erfassen.

> Dies alles betrifft natürlich nur Thin Clients, welche die Voraussetzungen für sicheres Spiegeln erfüllen und die entsprechende Option auch aktiviert haben. Andere Thin Clients lassen sich wie gehabt "frei" spiegeln, ggf. abgesichert durch die Abfrage eines Passworts. Möchten Sie ausschließlich sicheres Spiegeln erlauben, können Sie das in Zusätzliche Einstellungen im Administrationsbereich festlegen.

11.5.1. Grundlagen und Voraussetzungen

Die Option **Sicheres Spiegeln** ist unter folgenden Voraussetzungen aktivierbar:

- IGEL Universal Desktop Linux oder IGEL Universal Desktop OS 2 jeweils ab Version 5.03.190 bzw. IGEL Universal Desktop Windows Embedded Standard 7 ab Version 3.09.100
- IGEL Universal Management Suite ab Version 4.07.100
- Thin Client ist am UMS-Server registriert
- Thin Client kann mit UMS-Konsole und UMS-Server kommunizieren (s.u.)

Technische Grundlagen:

Im Gegensatz zum "normalen" Spiegeln wird beim sicheren Spiegeln die Verbindung zwischen VNC-Viewer und VNC-Server (auf dem Thin Client) nicht direkt aufgebaut, sondern läuft über zwei Proxies - einen seitens der UMS-Konsole und einen seitens des VNC-Servers auf dem Thin Client. Diese Proxies kommunizieren über einen SSL/TLS-verschlüsselten Kanal, während die lokale Kommunikation z.B. zwischen VNC-Viewer-Anwendung und UMS-Proxy herkömmlich unverschlüsselt erfolgt. Somit kann eine gesicherte Verbindung auch mit externen VNC-Programmen aufgebaut werden, die selbst keine SSL/TLS-Verbindung unterstützen.

Die beiden Proxies (UMS-Konsole und Thin Client) kommunizieren SSL/TLS-verschlüsselt über den gleichen Port wie die "normale" VNC-Verbindung: 5900. Somit müssen für das sichere Spiegeln keine gesonderten Regeln für Firewalls konfiguriert werden.

Ist das sichere Spiegeln für einen Thin Client aktiv (**Setup→System→Spiegeln→Sicheres Spiegeln**), generiert der Thin Client beim nächsten Systemstart ein Zertifikat nach X.509-Standard und übermittelt dieses an den UMS-Server. Dieser überprüft spätere Anfragen nach einer sicheren VNC-Verbindung anhand des Zertifikats. Das Zertifikat liegt im PEM-Format vor im Verzeichnis `/wfs/ca-certs/tc_ca.crt` auf dem Thin Client. Die Gültigkeit des Zertifikats lässt sich am (Linux) Thin Client prüfen mit dem Kommando:

```
x11vnc -sslCertInfo /wfs/ca-certs/tc_ca.crt
```

```
VNC Certificate file:
        /wfs/ca-certs/tc_ca.crt

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1572055243 (0x5db3a8cb)
    Signature Algorithm: md5WithRSAEncryption
        Issuer: C=DE, L=Bremen, O=IGEL
        Validity
            Not Before: Jun  6 06:04:50 2014 GMT
            Not After : Jun  6 06:04:50 2037 GMT
        Subject: C=DE, L=Bremen, O=IGEL
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:a4:e4:67:f3:cf:23:90:06:c3:d6
                    5e:0e:00:b8:43:14:6d:61:c5:65:ca
```

Figure 87: Thin Client Zertifikat für sicheres Spiegeln

Ruft ein UMS-Administrator in der UMS-Konsole für den Thin Client die Funktion **Spiegeln** auf, so erhält die Konsole vom UMS-Server eine signierte Anfrage, welche dann an den zu spiegelnden Thin Client weitergeleitet wird. Dieser wiederum leitet die Anfrage erneut an den UMS-Server weiter, der Anhand des ursprünglichen Zertifikats die Gültigkeit der Anfrage prüft und im Erfolgsfall der Konsole zurückmeldet, dass der Kanal für die Verbindung zwischen den Proxies aufgebaut werden kann. Der UMS-Proxy auf der Konsole verbindet sich zum Server-Proxy auf dem Thin Client, dieser wiederum baut auf dem Thin Client die Verbindung zu dessen VNC-Server auf.

Erst wenn diese Verbindungen aufgebaut sind, ruft die Konsole den VNC-Viewer auf, der sich mit dem Proxy der Konsole verbindet. Nun sind VNC-Client und VNC-Server über die beiden Proxies verbunden, die über SSL/TLS verschlüsselt übertragen.

> Das sichere Spiegeln kann unabhängig von der Thin Client Konfiguration für alle Thin Clients erzwungen werden, die diese Funktion unterstützen: **UMS Administration > Zusätzliche Einstellungen > Sicheres VNC global aktivieren**.

11.5.2. Thin Clients sicher spiegeln

Um einen Thin Client sicher (verschlüsselt) zu spiegeln, muss der Administrator sich über die UMS-Konsole am Server anmelden. Dabei ist es egal, ob ein rein lokales UMS-Administratorkonto verwendet wird oder der Benutzer z.B. über ein Active Directory übernommen wurde. Der UMS-Administrator muss aber wie üblich über das Recht zum Spiegeln des Objekt besitzen:

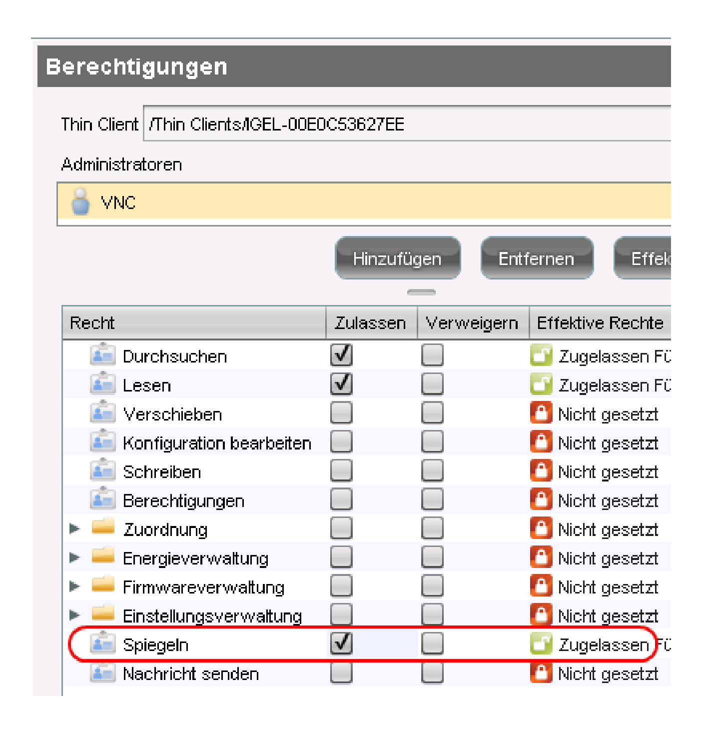


Figure 88: Administratorrecht Spiegeln

Der zu spiegelnde Thin Client wird im Navigationsbaum aufgerufen und wie üblich kann über das Kontextmenü der Punkt **Spiegeln** ausgeführt werden. Das Verbindungsfenster unterscheidet sich jedoch vom Dialog des normalen VNC-Spiegelns. Weder lassen sich IP und Port des zu spiegelnden Thin Clients ändern, noch wird ein Passwort für die Verbindung abgefragt - dies ist durch die zuvor erfolgte Konsolenanmeldung überflüssig.

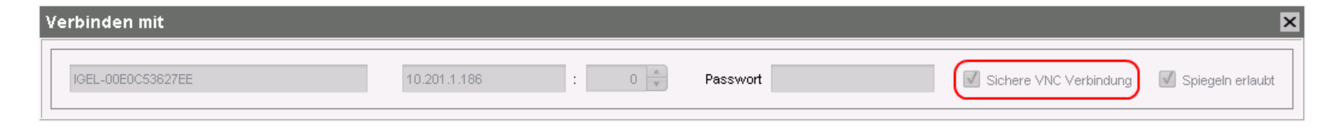


Figure 89: Verbindungsdialog Sicheres Spiegeln

Bei bestehender VNC-Verbindung erkennt man das sichere Spiegeln am Symbol des Verbindungsreiters:

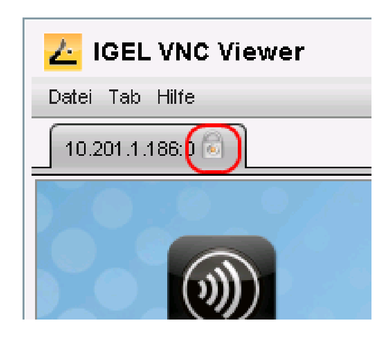


Figure 90: Sichere VNC-Verbindung

11.5.3. VNC-Logging

Verbindungen über das sichere Spiegeln werden grundsätzlich in der UMS protokolliert. Dabei lässt sich in **UMS-Administration→Zusätzliche Einstellungen→Sichere VNC-Verbindung** konfigurieren, ob der Benutzername des Spiegelnden in das Log aufgenommen werden soll (Vorgabe ist inaktiv):

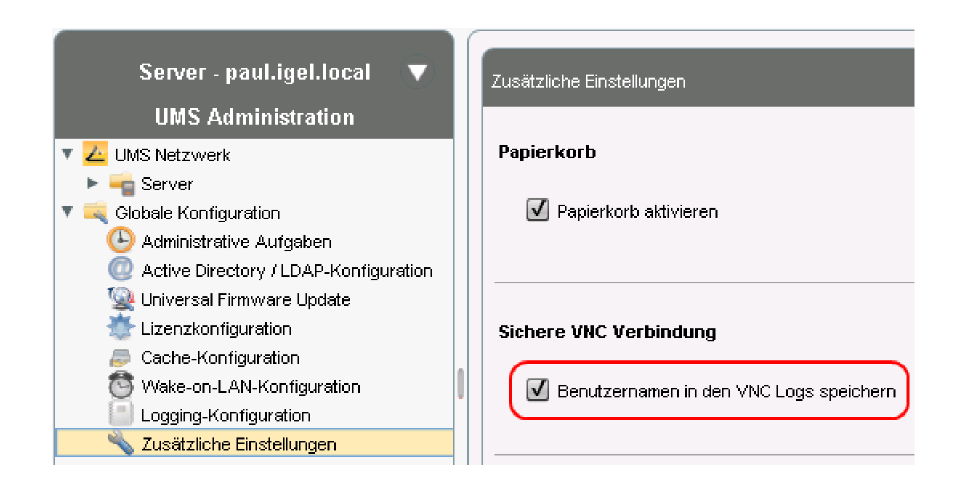
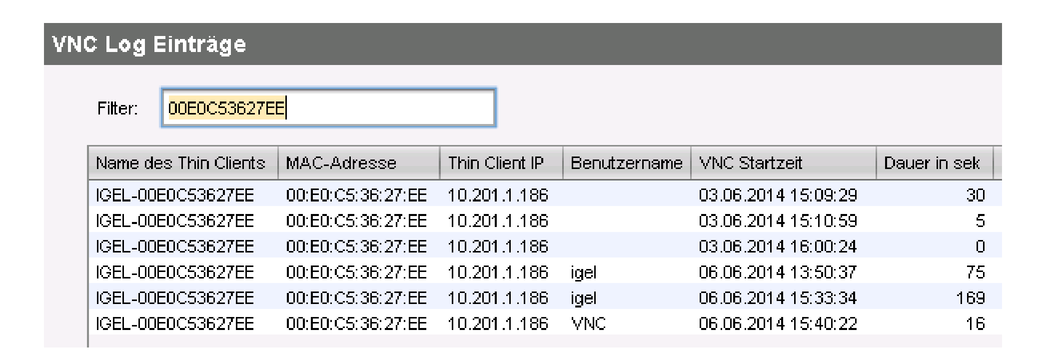


Figure 91: Optionen für VNC-Logging

Das VNC-Log lässt sich über das **Kontextmenü** eines Thin Clients oder eines Ordners (für mehrere Thin Clients) aufrufen (**Logging→VNC-Log**). Protokolliert werden Name, MAC-Adresse und IP-Adresse des gespiegelten Thin Clients, Zeitpunkt und Dauer des Vorgangs und ggf. der Benutzername des spiegelnden UMS-Administrators:



VNC Log Einträge

Filter: 00E0C53627EE

Name des Thin Clients	MAC-Adresse	Thin Client IP	Benutzername	VNC Startzeit	Dauer in sek
IGEL-00E0C53627EE	00:E0:C5:36:27:EE	10.201.1.186		03.06.2014 15:09:29	30
IGEL-00E0C53627EE	00:E0:C5:36:27:EE	10.201.1.186		03.06.2014 15:10:59	5
IGEL-00E0C53627EE	00:E0:C5:36:27:EE	10.201.1.186		03.06.2014 16:00:24	0
IGEL-00E0C53627EE	00:E0:C5:36:27:EE	10.201.1.186	igel	06.06.2014 13:50:37	75
IGEL-00E0C53627EE	00:E0:C5:36:27:EE	10.201.1.186	igel	06.06.2014 15:33:34	169
IGEL-00E0C53627EE	00:E0:C5:36:27:EE	10.201.1.186	VNC	06.06.2014 15:40:22	16

Figure 92: Logeinträge der sicheren VNC-Verbindungen

- Klicken Sie zum Sortieren der Liste (z.B. nach Benutzername) auf die entsprechende **Spaltenüberschrift** oder filtern Sie die angezeigten Inhalte durch Eingaben im Feld **Filter**.

11.6. Fernzugriff (SSH / RSH)

Um die zentrale Administration zu ermöglichen, kann der Thin Client so konfiguriert werden, dass über das WAN auf ihn zugegriffen werden kann.

Standardmäßig wird der Fernzugriff auf das lokale Setup gestattet. Sie können jedoch hier den Fernzugriff auf einen bestimmten Benutzer von einem bestimmten Host einschränken. Aktivieren Sie dazu die Einschränkung und geben Sie den vollständigen Namen des Hosts (z. B. `xterm.igel.de`) und den zulässigen Benutzer an.

11.7. Energie

Unter **System -> Energieoptionen** finden Sie im Setup zahlreiche Einstellungen für die Energieverwaltung.

11.7.1. Energie_System

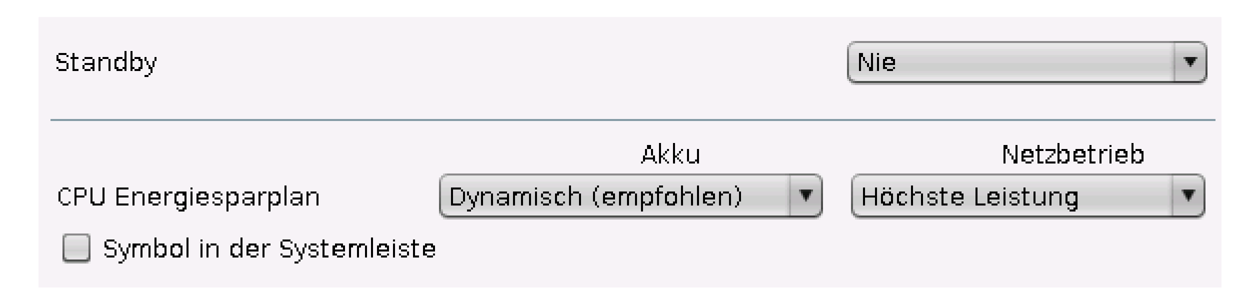


Figure 93: Energieoptionen System

Standby	Stellen Sie hier ein, nach wie langer Untätigkeit des Benutzers das System in den Standby-Zustand gehen soll, von **Nie** über **10 Min.** bis zu **24 Stunden**.
CPU Energiesparplan	Stellen Sie hier ein, welchen Energiesparplan für die CPU (CPU Governor) das Gerät im Netzbetrieb verwenden soll. Erläuterung der Einstellungen: • **Höchste Leistung** - volle Leistung durch höchsten Prozessortakt • **Dynamisch (sanft)** - langsamere, ausgeglichene Anpassung der Leistung an die Anforderungen der Programme. Geeignet für Benutzer, die häufiges Hochdrehen des Lüfters stört. • **Dynamisch (empfohlen)**- rasche Anpassung der Leistung an die Anforderungen der Programme (empfohlen) • **Energie sparen**- niedrigster Prozessortakt Die Standardeinstellungen sind **Höchste Leistung** im Netzbetrieb und **Dynamisch (empfohlen)** im Batteriebetrieb.
Symbol in der Systemleiste	Aktivieren Sie diese Einstellung, um ein CPU-Symbol in der Systemleiste anzuzeigen, über das sich die Energiesparpläne rasch wechseln lassen.

11.7.2. Akku

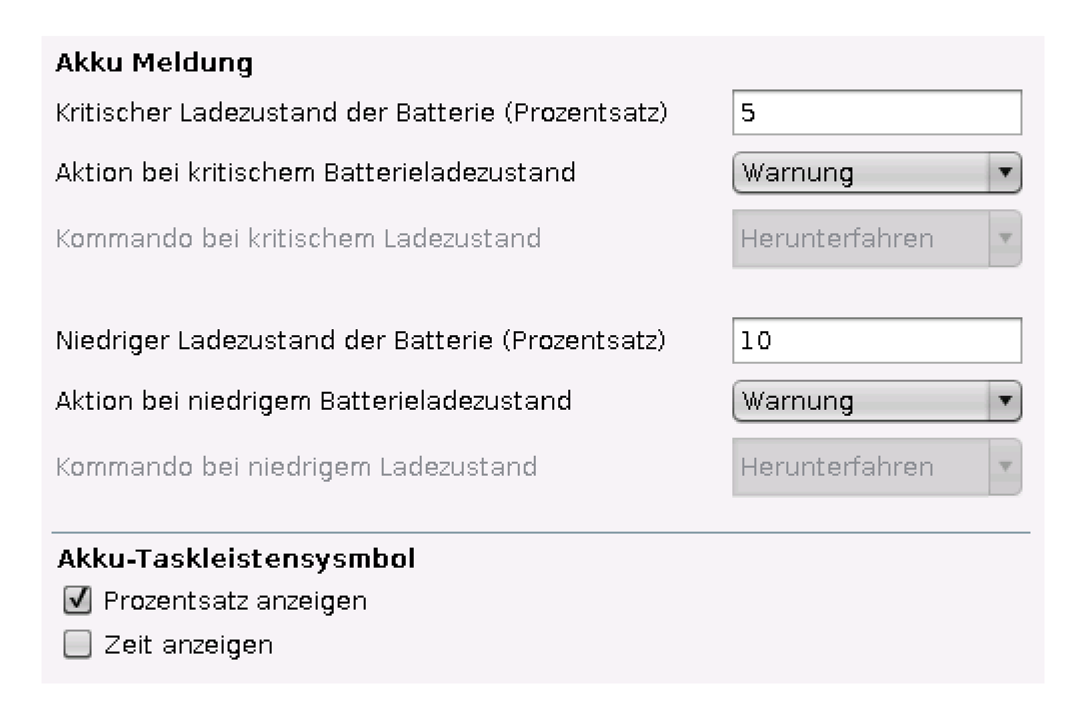


Figure 94: Energieoptionen Akku

Kritischer Ladezustandstand der Batterie (Prozentsatz)	Hier konfigurieren Sie, ab welchem Prozentsatz der Ladezustand der Batterie als kritisch gelten soll. Sie können zwei verschiedene Szenarien konfigurieren.
Aktion bei kritischem Batterieladezustand	Hier stellen Sie ein, welche Aktion bei kritischem Batterieladezustand erfolgen soll: **Keine Aktion, Warnung, Kommando ausführen** oder **Kommando in Konsole ausführen**.
Kommando bei kritischem Ladezustand	Geben Sie hier ein gültiges Kommando ein. Das Standardkommando `user_shutdown -f` fährt das System ordnungsgemäß herunter.
Prozentsatz anzeigen	Zeigt den Prozentsatz der Batterieladung im Tray an.
Zeit anzeigen	Zeigt die verbleibende Batterielaufzeit- / -ladezeit im Tray an

11.7.3. Bildschirm

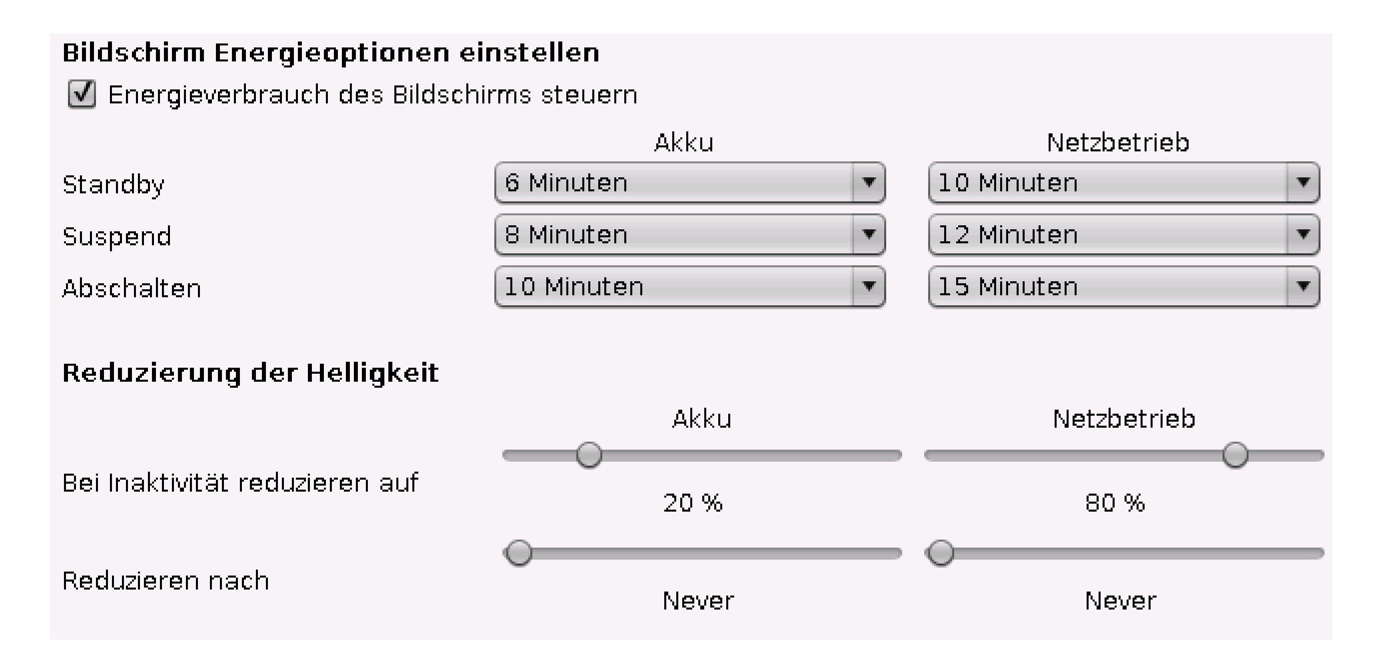


Figure 95: Energieoptionen Bildschirm

Bildschirm Energieoptionen einstellen

Energieverbrauch des Bildschirms steuern	Aktivieren Sie dieses Kontrollkästchen um die folgenden Einstellungen vornehmen zu können. In älteren Firmwares hieß diese Option DPMS (Display Power Management Signaling).
Standby	Bestimmen Sie, nach wie vielen Minuten Untätigkeit des Benutzers der Bildschirm in den Standbymodus schalten soll.
Suspend	Bestimmen Sie, nach wie vielen Minuten der Bildschirm in den Suspendmodus schalten soll.
Abschalten	Bestimmen Sie, nach wie vielen Minuten der Bildschirm sich abschalten soll.

Reduzierung der Helligkeit

Bei Inaktivität reduzieren auf	Legen Sie fest auf wieviel Prozent der Helligkeit der Bildschirm reduziert werden soll, wenn sie das Gerät nicht nutzen.
Reduzieren nach	Legen Sie eine Zeit zwischen10 und 120 Sekunden fest, nach der die Helligkeitsreduzierung des Bildschirms starten soll.

11.7.4. Herunterfahren

Diese Setupseite enthält Einstellungen für das Herunterfahren.

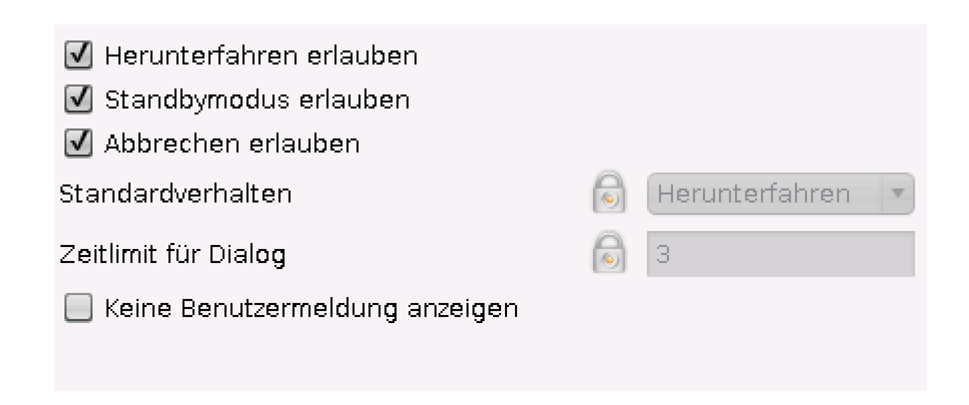


Figure 96: Herunterfahren

Herunterfahren erlauben	Erlaubt dem Anwender, das Gerät herunterzufahren.
Standbymodus erlauben	Erlaubt dem Anwender, das Gerät in den Standbymodus zu versetzen.
Abbrechen erlauben	Erlaubt dem Anwender, das Herunterfahren oder in den Standby Versetzen abzubrechen.
Standardverhalten	Definiert, welches Verhalten im angezeigten Dialog vorausgewählt ist.
Zeitlimit für Dialog	Zeitspanne in Sekunden, nachdem die im Dialog vorausgewählte Option ausgeführt wird.
Keine Benutzermeldung anzeigen	Beim Herunterfahren keinen Dialog anzeigen, mit dem der Benutzer interagieren kann.

11.7.5. Energieoptionen

Die Setupseite **System-> Energie->Energieoptionen** bietet zahlreiche Einstellungen für die Energieverwaltung.



Figure 97: Standby

Standby	Stellen Sie hier ein, nach wie langer Untätigkeit des Benutzers das System in den Standby-Zustand gehen soll, von **Nie** über **10 Min.** bis zu **24 Stunden**.

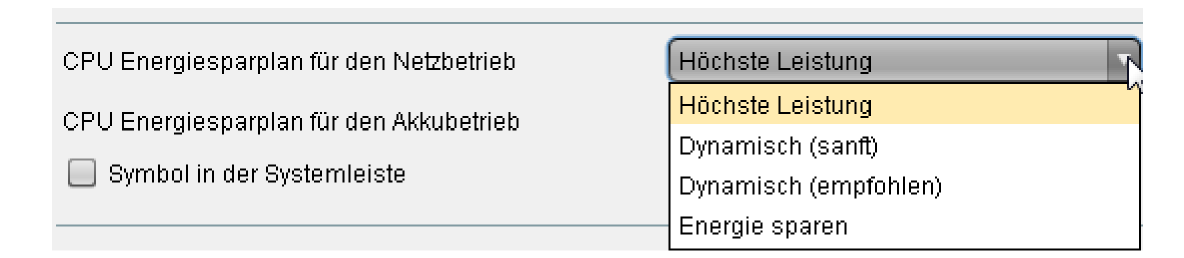


Figure 98: CPU

CPU Energiesparplan für den Netzbetrieb	Stellen Sie hier ein, welchen Energiesparplan für die CPU (CPU Governor) das Gerät im Netzbetrieb verwenden soll. Erläuterung der Einstellungen: • **Höchste Leistung** - volle Leistung durch höchsten Prozessortakt • **Dynamisch (sanft)** - langsamere, ausgeglichene Anpassung der Leistung an die Anforderungen der Programme. Geeignet für Benutzer, die häufiges Hochdrehen des Lüfters stört. • **Dynamisch (empfohlen)**- rasche Anpassung der Leistung an die Anforderungen der Programme (empfohlen) • **Energie sparen**- niedrigster Prozessortakt Die Standardeinstellungen sind **Höchste Leistung** im Netzbetrieb und **Dynamisch (empfohlen)** im Batteriebetrieb.
CPU Energiesparplan für den Batteriebetrieb	Stellen Sie hier ein, welchen Energiesparplan für die CPU (CPU Governor) das Gerät im Batteriebetrieb verwenden soll. Erläuterung der Einstellungen siehe oben.
Symbol in der Systemleiste	Aktivieren Sie diese Einstellung, um ein CPU-Symbol in der Systemleiste anzuzeigen, über das sich die Energiesparpläne rasch wechseln lassen.

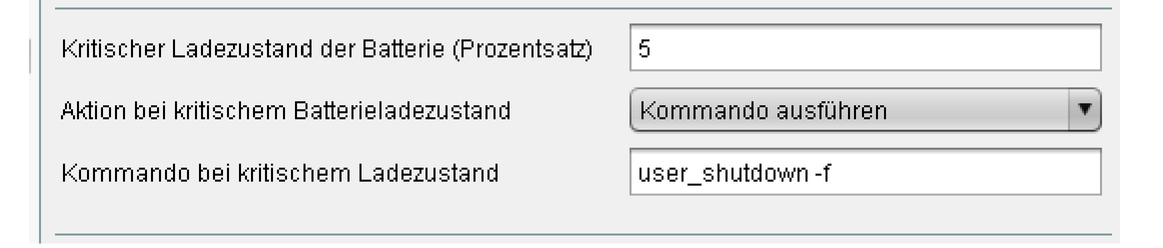


Figure 99: Kritischer Ladezustand

Kritischer Ladezustandstand der Batterie (Prozentsatz)	Hier konfigurieren Sie, ab welchem Prozentsatz der Ladezustand der Batterie als kritisch gelten soll.
Aktion bei kritischem Batterieladezustand	Hier stellen Sie ein, welche Aktion bei kritischem Batterieladezustand erfolgen soll: **Keine Aktion**, **Warnung**, **Kommando ausführen** oder **Kommando in Konsole ausführen**.
Kommando bei kritischem Ladezustand	Geben Sie hier ein gültiges Kommando ein. Das Standardkommando `user_shutdown -f` fährt das System ordnungsgemäß herunter.



Figure 100: Niedriger Ladezustand

Niedriger Ladezustandstand der Batterie (Prozentsatz)	Hier konfigurieren Sie, ab welchem Prozentsatz der Ladezustand der Batteire als niedrig gelten soll.
Aktion bei niedrigem Batterieladezustand	Hier stellen Sie ein, welche Aktion bei niedrigem Batterieladezustand erfolgen soll: **Keine Aktion**, **Warnung**, **Kommando ausführen** oder **Kommando in Konsole ausführen.**
Kommando bei niederigem Ladezustand	Geben Sie hier ein gültiges Kommando ein. Das Standardkommando `user_shutdown -f` fährt das System ordnungsgemäß herunter.

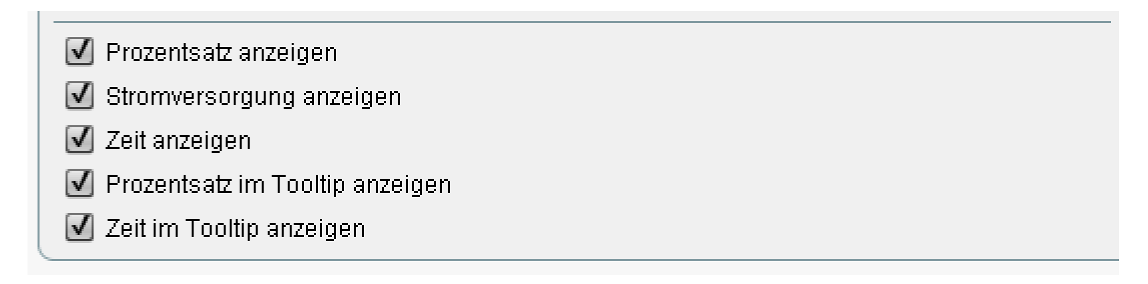


Figure 101: Optionen

Prozentsatz anzeigen	Zeigt den Prozentsatz der Batterieladung im Tray an.
Stromversorgung anzeigen	Zeigt im Tray an, ob ein Netzteil zur Stromversorgung angeschlossen ist.
Zeit anzeigen	Zeigt die verbleibende Batterielaufzeit- / -ladezeit im Tray an
Prozentsatz im Tooltipp anzeigen	Zeigt den Prozentsatz der Batterieladung als Tooltipp an.
Zeit im Tooltipp anzeigen	Zeigt die verbleibende Batterielaufzeit- / -ladezeit im Tooltipp an.

11.7.6. DPMS

Per DPMS (Display Power Management Signaling) können Sie Ihrem Bildschirm Signale zur Energieverwaltung schicken, falls er es unterstützt.

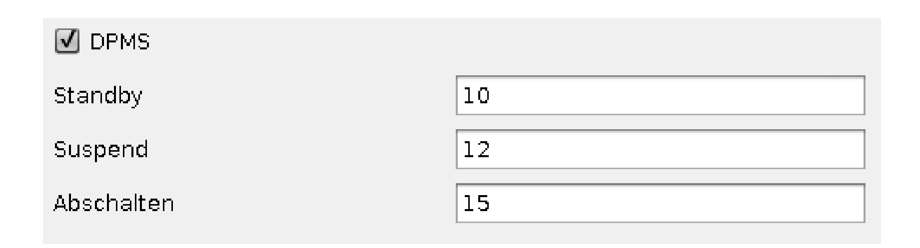


Figure 102: DPMS

DPMS	Aktivieren Sie DPMS.
Standby	Nach wie vielen Minuten Untätigkeit des Benutzers der Bildschirm in den Standbymodus schalten soll.
Suspend	Nach wie vielen Minuten der Bildschirm in den Suspendmodus schalten soll.
Ausschalten	Nach wie vielen Minuten der Bildschirm sich ausschalten soll

11.8. Anpassung der Firmware

Gestalten Sie die Firmware um zu Ihrem ganz persönlichen Arbeitsplatz.

11.8.1. Eigene Anwendungen

Anwendungen, die z. B. in eine Kundenpartition geladen wurden, lassen sich nach Definition einer eigenen Anwendung über den **Starter für Sitzungen** bzw. über ein Icon auf der Arbeitsfläche starten. Dazu wird das Kommando zum Aufruf der Anwendung unter **Einstellungen** eingetragen.

11.8.2. Eigene Kommandos

Eigene Kommandos (**Custom Commands**) lassen sich zu verschiedenen Zeitpunkten beim Systemstart einhängen. Diese Kommandos können *konfigurierte Umgebungsvariablen* (Seite 138) benutzen.

Basiskommandos laufen einmalig beim Bootvorgang.

Die Ausführungszeitpunkte sind:

Initialisierung	Nicht alle Treiber geladen, nicht alle Geräte verfügbar Netzwerkskripte nicht gestartet, Netzwerk nicht verfügbar Partitionen verfügbar außer firefox profile, scim data, ncp data, custom partition
Sitzung Start	Nicht alle Treiber geladen, nicht alle Geräte verfügbar Netzwerkskripte gestartet, Netzwerk nicht verfügbar Partitionen verfügbar außer firefox profile, scim data, ncp data, custom partition Sitzungen nicht konfiguriert
Sitzung Ende	Alle Treiber geladen, alle Geräte verfügbar Netzwerk verfügbar Partitionen verfügbar außer custom partition System Daemons nicht gestartet (CUPS, ThinPrint u.a.) Sitzungen konfiguriert UMS-Einstellungen abgerufen aber noch nicht wirksam
Ende	Alle Partitionen verfügbar Alle System Daemons gestartet UMS-Einstellungen wirksam

Netzwerkkommandos laufen bei jedem Netzwerkstart des betreffenden Interfaces (Standard `eth0`). Das Interface kann mit der Umgebungsvariablen `$INTERFACE` gewählt werden (`eth0`, `eth1`, `wlan0`).

Die Ausführungszeitpunkte sind:

Netzwerk Initialisierung	Netzwerkauthentifizierung erfolgreich (802.1x bzw. WPA) Keine weiteren Netzwerkeinstellungen angewendet
Netzwerk DNS	Läuft nach jeder Änderung von IP-Adresse oder Hostname IP-Adresse / Nameserver Einstellungen angewendet (z.B. über DHCP)
Netzwerk Start	IP-Adresse / Nameserver Einstellungen angewendet VPN verbunden (falls VPN-Autostart im Setup aktiviert wurde) Keine Netzwerk / Host Routing Einstellungen angewendet
Netzwerk Ende	Netzwerk / Host Routing Einstellungen angewendet NFS- und SMB-Laufwerke verfügbar Systemzeit mit Zeitserver synchronisiert UMS-Einstellungen abgerufen aber noch nicht wirksam

Arbeitsflächenkommados laufen beim Start des X Servers.

Die Ausführungszeitpunkte sind:

Arbeitsfläche Initialisierung	Läuft einmalig beim Bootvorgang Desktopumgebung konfiguriert aber nicht gestartet Benutzer nicht angemeldet (Kerberos, Smartcard usw.)
Arbeitsfläche Start	Läuft einmalig beim Bootvorgang Desktopumgebung gestartet Benachrichtigungsdienst gestartet Session D-Bus gestartet Benutzer nicht angemeldet (Kerberos, Smartcard usw.)
Arbeitsfläche Ende	Läuft nach jeder Benutzeranmeldung und Neustart des Desktops Benutzer angemeldet (Kerberos, Smartcard usw.) Benutzerarbeitsfläche gestartet

Neukonfigurationskommandos laufen bei geänderten Einstellungen über das lokale Setup oder die UMS.

Die Ausführungszeitpunkte sind:

Neukonfiguration	Läuft nach wirksamer Änderung der Thin Client Einstellungen (lokales Setup, UMS)

11.8.3. Startbildschirm (Bootsplash) anpassen

Siehe Beschreibung in Kapitel *Benutzeroberfläche* (Seite 78).

11.8.4. Umgebungsvariablen

Umgebungsvariablen erlauben den Einsatz dynamischer Parameterinhalte für einige Sitzungstypen, z. B. um ICA- oder RDP-Server nicht für jede Sitzung eintragen zu müssen. Im IGEL Setup sind die Variablen zu finden unter: **System→Firmware Anpassung→Umgebungsvariablen**

Vordefinierte Variablen können auch über die IGEL UMS belegt und verteilt werden, zusätzlich definierte Variablen können nur lokal verwendet werden und werden ggf. von einer UMS-Konfiguration überschrieben.

Die Umgebungsvariablen stehen in *Eigene Kommandos* (Seite 136) zur Verwendung bereit.

Daneben lassen sich folgende Sitzungsparameter können durch Variablen pflegen:

- ICA - Username (ICA Sitzungen→[Sitzungsname]→Logon)
- ICA - Citrix-Server bzw. Published Application (ICA Sitzungen→[Sitzungsname] -→ Server)
- XenApp - Username (Citrix XenApp/Program Neighborhood→Logon)
- RDP - Username (RDP Sitzungen→[Sitzungsname]→Logon)
- RDP - Server (RDP Sitzungen→[Sitzungsname]→Server)

Verwendung in Sitzungen

1. Aktivieren Sie die Umgebungsvariablen unter **Variablensubstitution in Sitzungen erlauben**.
2. Definieren Sie Variablenname und -inhalt (z. B. Variable Name = SERVERNAME | Value = testServer)
3. Tragen Sie den Variablennamen im Parameterfeld der Sitzung ein, dabei wird das Zeichen $ vorangestellt (z. B. wird bei einer RDP-Sitzung für den Server eingetragen: $SERVERNAME)

Für RDP- und ICA-Sitzungen wird nach dem Speichern der Einstellung die umgesetzt und in das Session File eingetragen. Bei XenApp wird dies erst zur Laufzeit beim Start der Sitzung umgesetzt.

11.8.5. Features

Über diese Liste der verfügbaren Services können Sie Firmwarebestandteile wie Powerterm, Media Player usw. schnell aktivieren oder deaktivieren. Wenn ein Service deaktiviert wurde, steht der zugehörige Sitzungstyp nach dem Neustart nicht mehr zur Verfügung. Bereits bestehende Sitzungen werden nicht angezeigt, aber auch nicht gelöscht. Ein deaktivierter Sitzungstyp wird während eines Firmwareupdates nicht aktualisiert. Um Updatevorgänge zu beschleunigen, sollten Sie daher ungenutzte Services deaktivieren.

> Hinweis: Ab Version 5.06.100 bietet IGEL Linux Hardwarebschleunigung für die Wiedergabe von Multimedia-Inhalten. Sie ist allerdings standardmäßig deaktiviert und unter dem Setup-Punkt **Features** aktivierbar. Details zur Hardwarebschleunigung finden Sie *in einem FAQ-Dokument.* (*http://edocs.igel.com/#10201440.htm*)

11.9. Registry

Sie können nahezu jeden Parameter der Firmware in der Registry ändern. Informationen zu den einzelnen Elementen finden Sie in den Tooltips.

Änderungen an der Thin Client-Konfiguration über die Registry sollten nur von erfahrenen Administratoren vorgenommen werden. Falsche Parametereinstellungen können leicht die Konfiguration zerstören und zu einem Systemabsturz führen. Die einzige Möglichkeit zur Wiederherstellung des Thin Clients ist in einem solchen Fall das Zurücksetzen auf die Werkseinstellungen!

Sie können in der IGEL Registry nach Setupparametern suchen, indem Sie auf die Schaltfläche **Parametersuche** klicken. Wenn Sie die FTP-Einstellungen für die Aktualisierung der Linux-Firmware finden möchten, können Sie nach dem Parameternamen ftp suchen. Der in der Registry-Struktur gefundene Parameter wird hervorgehoben:

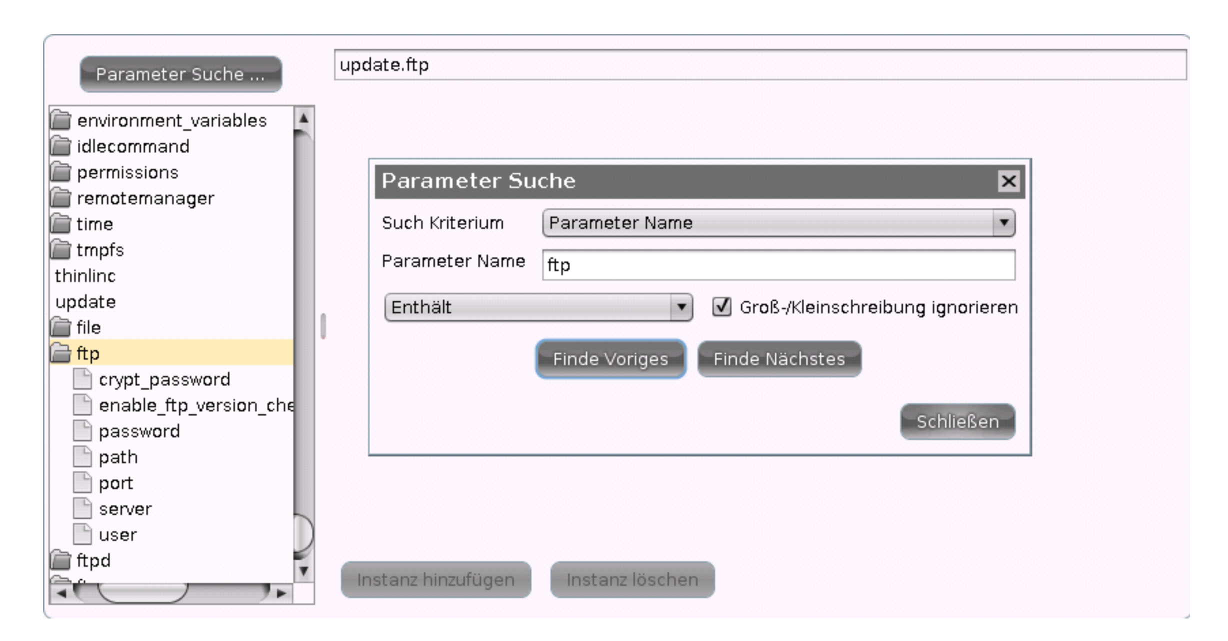


Figure 103: Parametersuche in der IGEL-Registry

12. Index

W

X

Z